FIG. 1

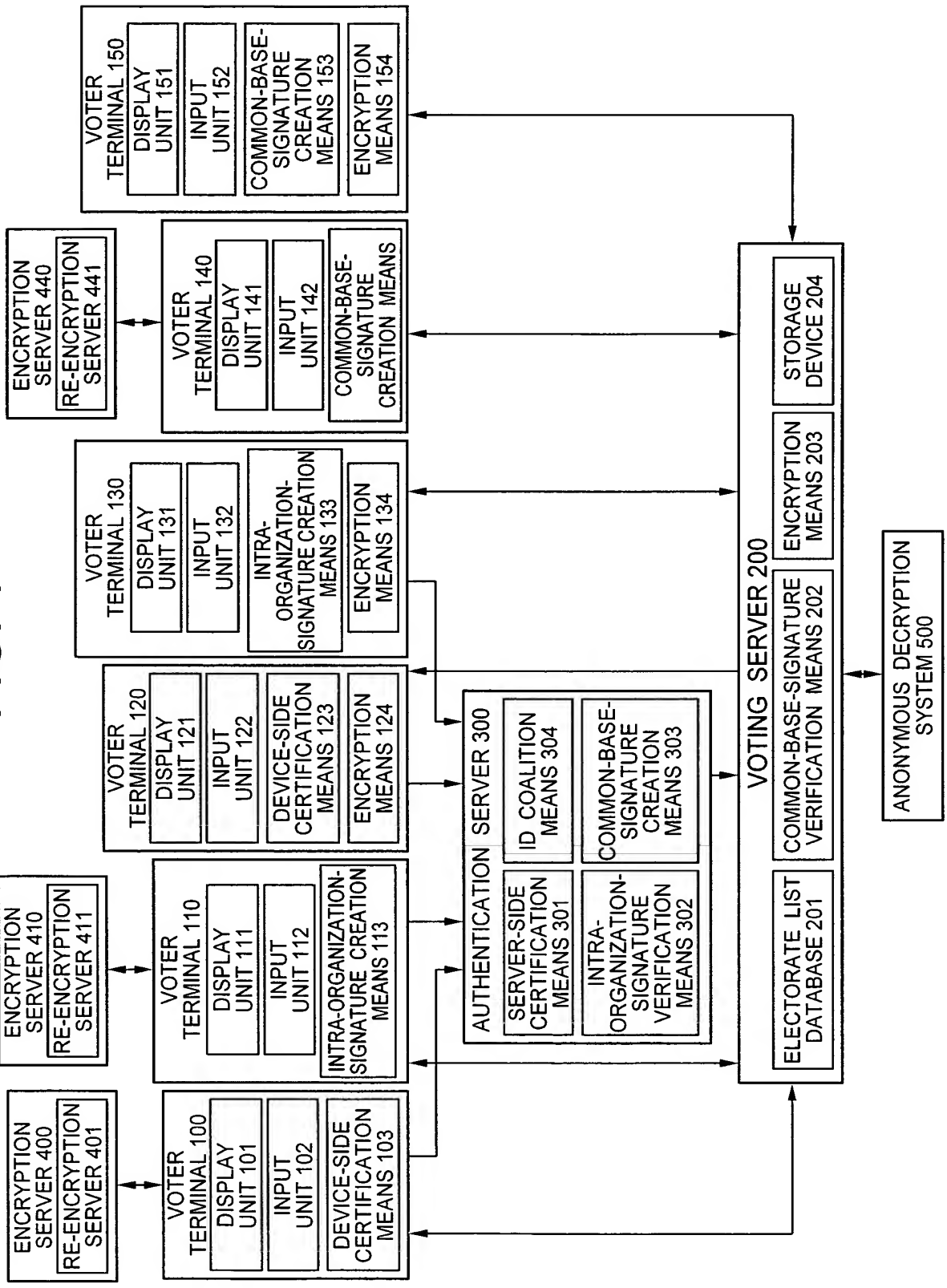

VOTER TERMINAL 150
DISPLAY UNIT 151
INPUT UNIT 152
COMMON-BASE-SIGNATURE CREATION MEANS 153
ENCRYPTION MEANS 154
ENCRYPTION SERVER 440
RE-ENCRYPTION SERVER 441
VOTER TERMINAL 140
DISPLAY UNIT 141
INPUT UNIT 142
COMMON-BASE-SIGNATURE CREATION MEANS
VOTER TERMINAL 130
DISPLAY UNIT 131
INPUT UNIT 132
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 133
ENCRYPTION MEANS 134
VOTER TERMINAL 120
DISPLAY UNIT 121
INPUT UNIT 122
DEVICE-SIDE CERTIFICATION MEANS 123
ENCRYPTION MEANS 124
ENCRYPTION SERVER 410
RE-ENCRYPTION SERVER 411
VOTER TERMINAL 110
DISPLAY UNIT 111
INPUT UNIT 112
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 113
ENCRYPTION SERVER 400
RE-ENCRYPTION SERVER 401
VOTER TERMINAL 100
DISPLAY UNIT 101
INPUT UNIT 102
DEVICE-SIDE CERTIFICATION MEANS 103
AUTHENTICATION SERVER 300
ID COALITION MEANS 304
SERVER-SIDE CERTIFICATION MEANS 301
COMMON-BASE-SIGNATURE CREATION MEANS 303
INTRA-ORGANIZATION-SIGNATURE VERIFICATION MEANS 302
VOTING SERVER 200
STORAGE DEVICE 204
ENCRYPTION MEANS 203
COMMON-BASE-SIGNATURE VERIFICATION MEANS 202
ELECTORATE LIST DATABASE 201
ANONYMOUS DECRYPTION SYSTEM 500

FIG. 2

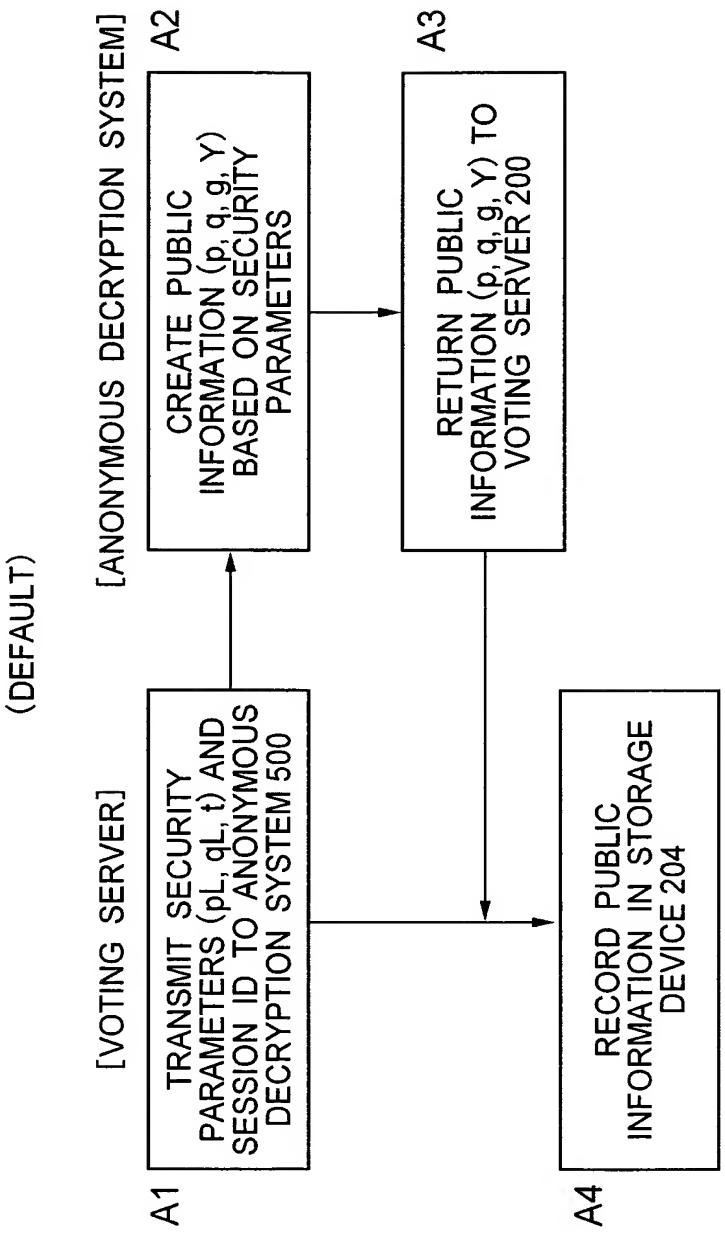

(DEFAULT)
[VOTING SERVER]
[ANONYMOUS DECRYPTION SYSTEM]
A1
TRANSMIT SECURITY PARAMETERS (pL, qL, t) AND SESSION ID TO ANONYMOUS DECRYPTION SYSTEM 500
A2
CREATE PUBLIC INFORMATION (p, q, g, Y) BASED ON SECURITY PARAMETERS
A3
RETURN PUBLIC INFORMATION (p, q, g, Y) TO VOTING SERVER 200
A4
RECORD PUBLIC INFORMATION IN STORAGE DEVICE 204

FIG. 3

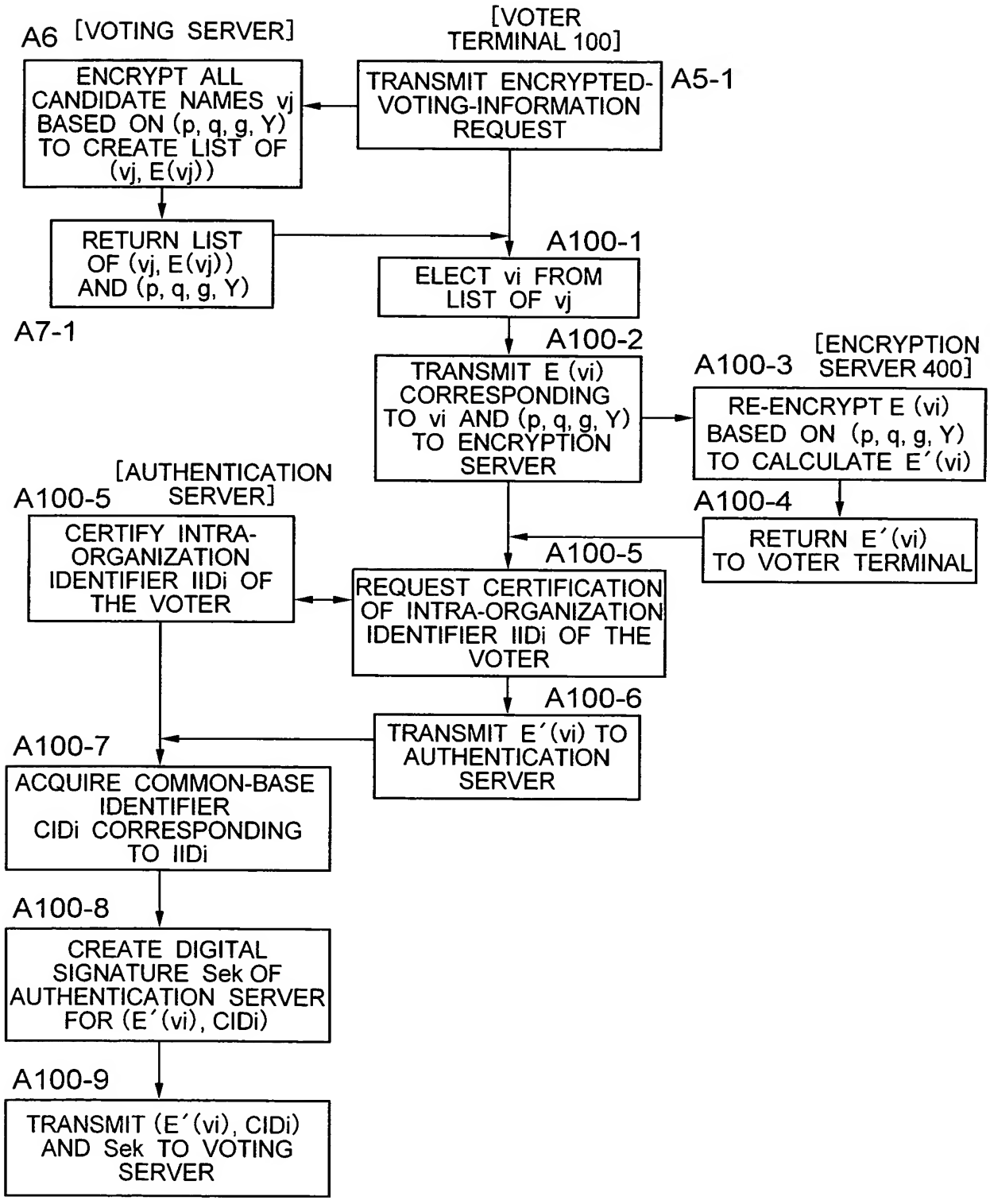

A6 [VOTING SERVER]
[VOTER TERMINAL 100]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y)
A7-1
A100-1
ELECT vi FROM LIST OF vj
A100-2
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
A100-3
[ENCRYPTION SERVER 400]
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E'(vi)
A100-4
RETURN E'(vi) TO VOTER TERMINAL
[AUTHENTICATION SERVER]
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-5
REQUEST CERTIFICATION OF INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-6
TRANSMIT E'(vi) TO AUTHENTICATION SERVER
A100-7
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A100-8
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E'(vi), CIDi)
A100-9
TRANSMIT (E'(vi), CIDi) AND Sek TO VOTING SERVER

FIG. 4

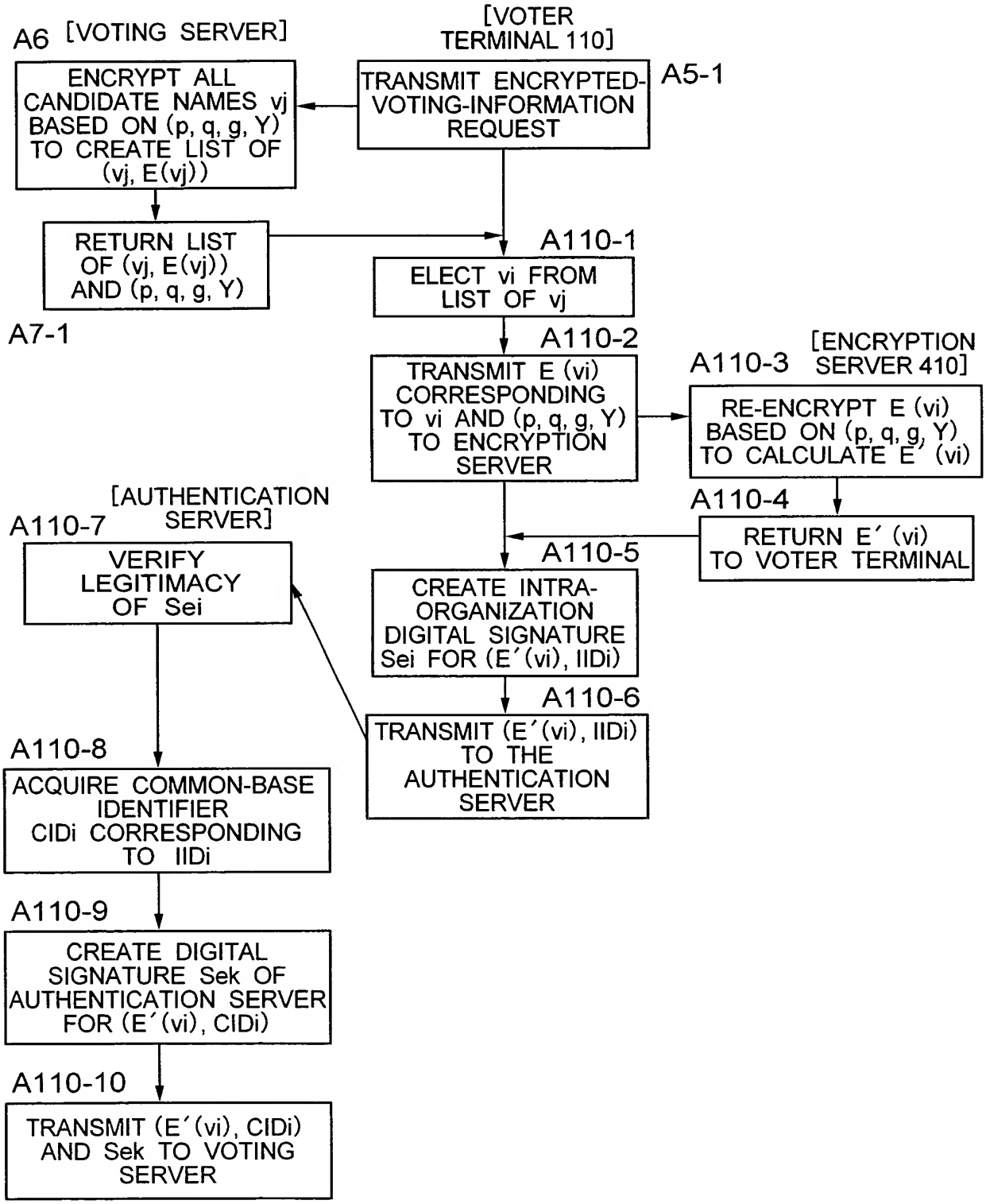

A6 [VOTING SERVER]
[VOTER TERMINAL 110]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y)
A7-1
A110-1
ELECT vi FROM LIST OF vj
A110-2
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
A110-3
[ENCRYPTION SERVER 410]
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E´ (vi)
A110-4
RETURN E´ (vi) TO VOTER TERMINAL
A110-5
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E´(vi), IIDi)
A110-6
TRANSMIT (E´(vi), IIDi) TO THE AUTHENTICATION SERVER
[AUTHENTICATION SERVER]
A110-7
VERIFY LEGITIMACY OF Sei
A110-8
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A110-9
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E´(vi), CIDi)
A110-10
TRANSMIT (E´(vi), CIDi) AND Sek TO VOTING SERVER

FIG. 5

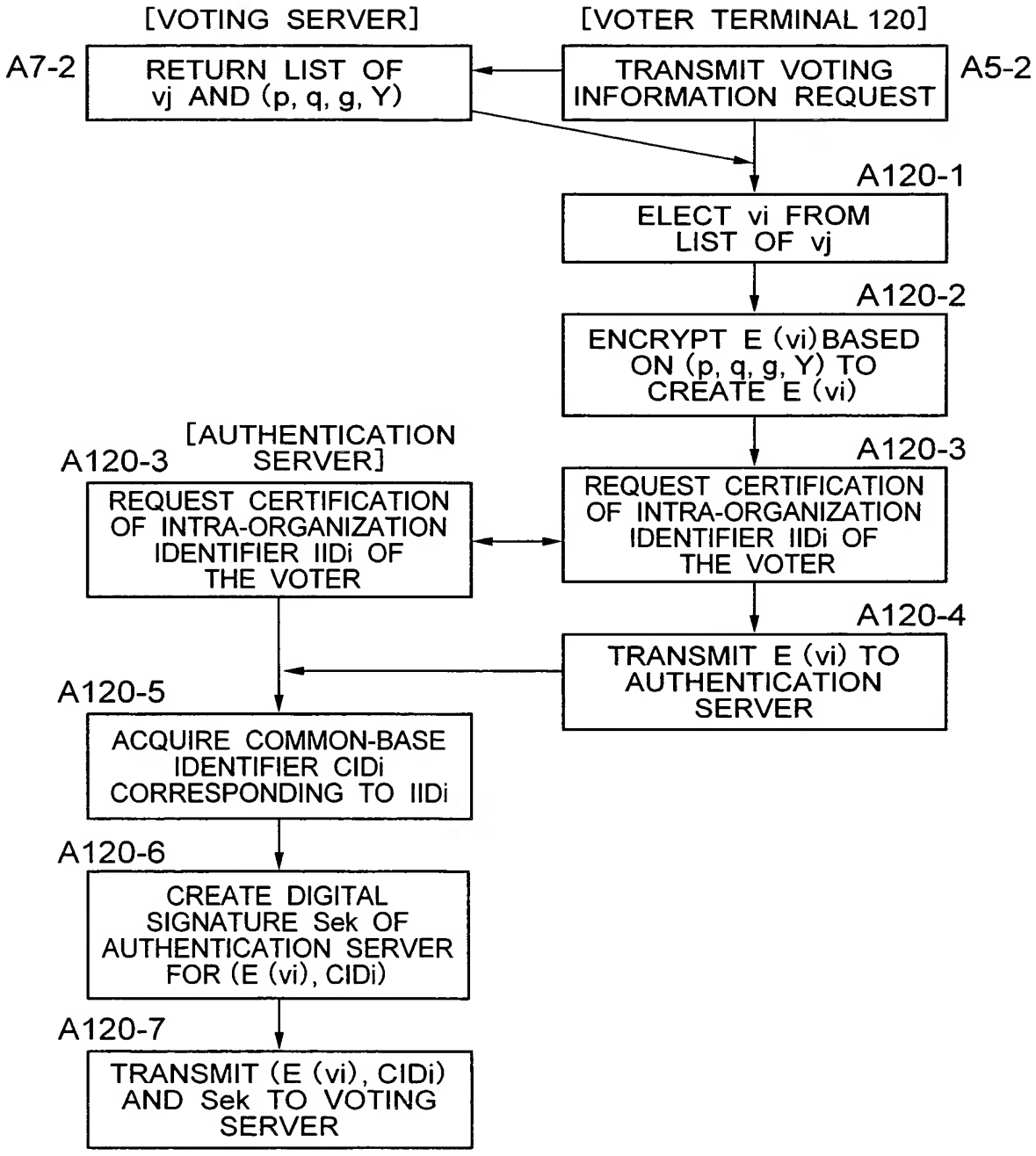

[VOTING SERVER]
[VOTER TERMINAL 120]
A7-2
RETURN LIST OF vj AND (p, q, g, Y)
TRANSMIT VOTING INFORMATION REQUEST
A5-2
A120-1
ELECT vi FROM LIST OF vj
A120-2
ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CREATE E (vi)
[AUTHENTICATION SERVER]
A120-3
REQUEST CERTIFICATION OF INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A120-3
REQUEST CERTIFICATION OF INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A120-4
TRANSMIT E (vi) TO AUTHENTICATION SERVER
A120-5
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A120-6
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E (vi), CIDi)
A120-7
TRANSMIT (E (vi), CIDi) AND Sek TO VOTING SERVER

FIG. 6

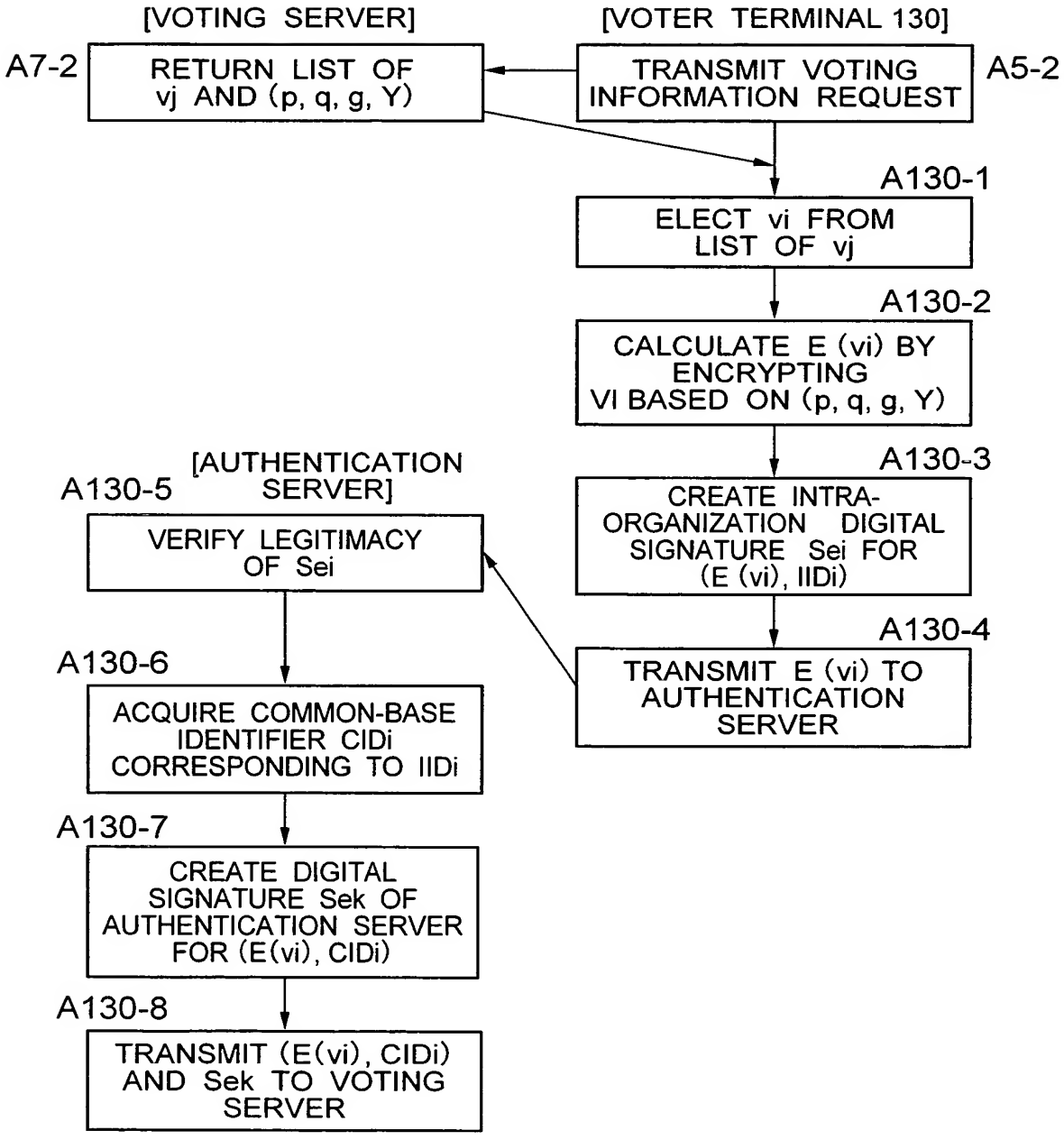

[VOTING SERVER]
[VOTER TERMINAL 130]
A7-2
RETURN LIST OF vj AND (p, q, g, Y)
TRANSMIT VOTING INFORMATION REQUEST
A5-2
A130-1
ELECT vi FROM LIST OF vj
A130-2
CALCULATE E (vi) BY ENCRYPTING VI BASED ON (p, q, g, Y)
A130-3
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E (vi), IIDi)
A130-4
TRANSMIT E (vi) TO AUTHENTICATION SERVER
[AUTHENTICATION SERVER]
A130-5
VERIFY LEGITIMACY OF Sei
A130-6
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A130-7
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E(vi), CIDi)
A130-8
TRANSMIT (E(vi), CIDi) AND Sek TO VOTING SERVER

FIG. 7

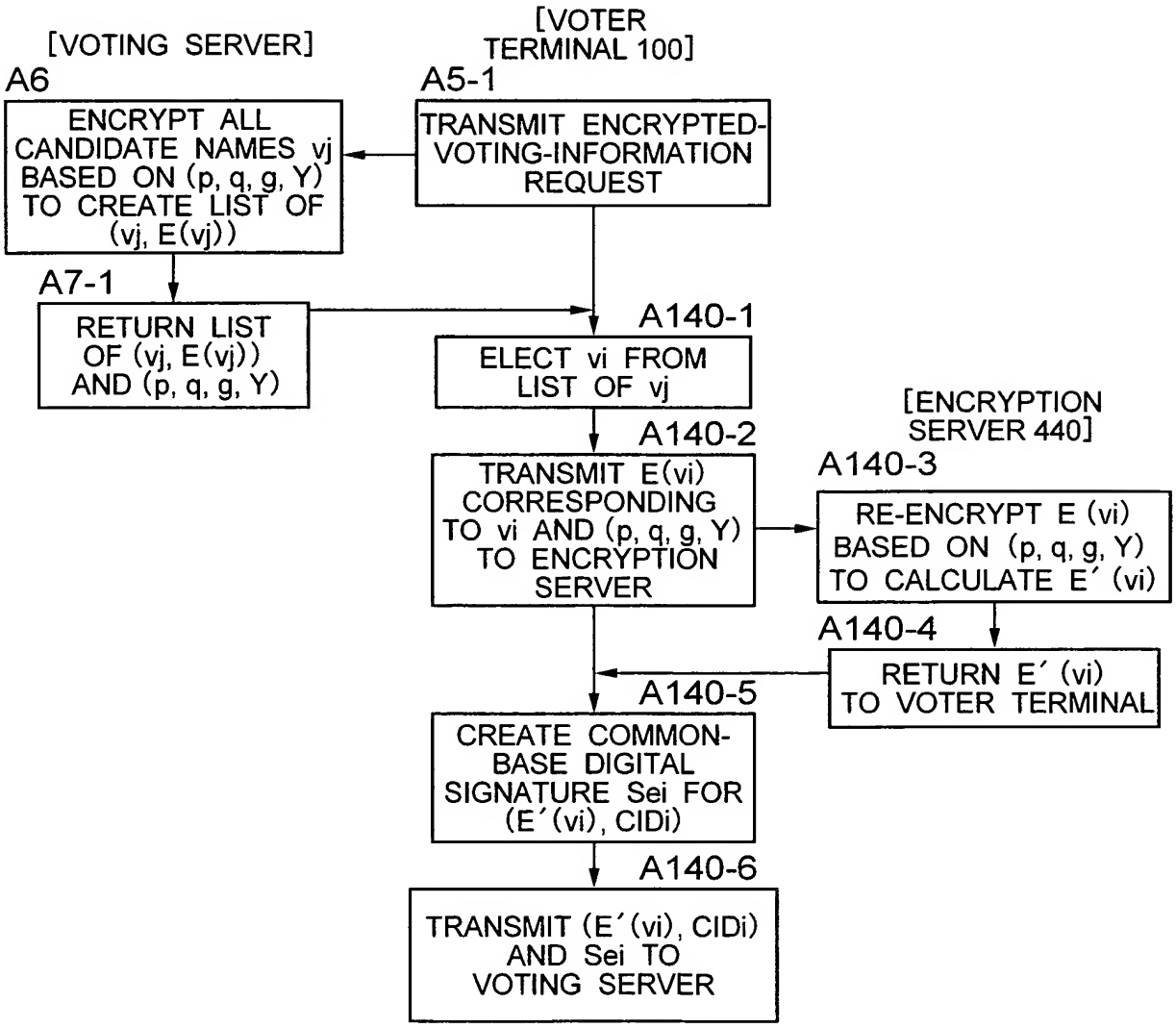

[VOTING SERVER]
[VOTER TERMINAL 100]
A6
A5-1
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A7-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y)
A140-1
ELECT vi FROM LIST OF vj
A140-2
TRANSMIT E(vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 440]
A140-3
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E′ (vi)
A140-4
RETURN E′ (vi) TO VOTER TERMINAL
A140-5
CREATE COMMON-BASE DIGITAL SIGNATURE Sei FOR (E′(vi), CIDi)
A140-6
TRANSMIT (E′(vi), CIDi) AND Sei TO VOTING SERVER

FIG. 8

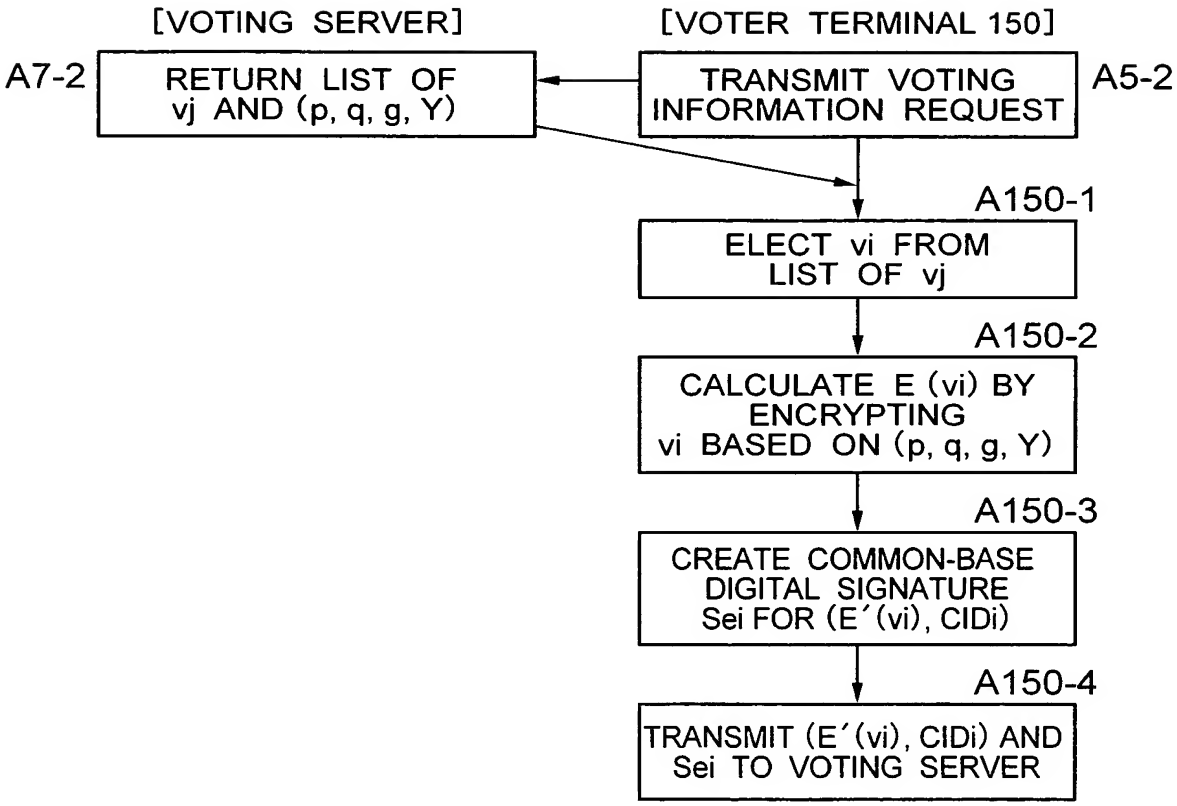

[VOTING SERVER]
[VOTER TERMINAL 150]
A7-2
RETURN LIST OF vj AND (p, q, g, Y)
TRANSMIT VOTING INFORMATION REQUEST
A5-2
A150-1
ELECT vi FROM LIST OF vj
A150-2
CALCULATE E (vi) BY ENCRYPTING vi BASED ON (p, q, g, Y)
A150-3
CREATE COMMON-BASE DIGITAL SIGNATURE Sei FOR (E'(vi), CIDi)
A150-4
TRANSMIT (E'(vi), CIDi) AND Sei TO VOTING SERVER

FIG. 9

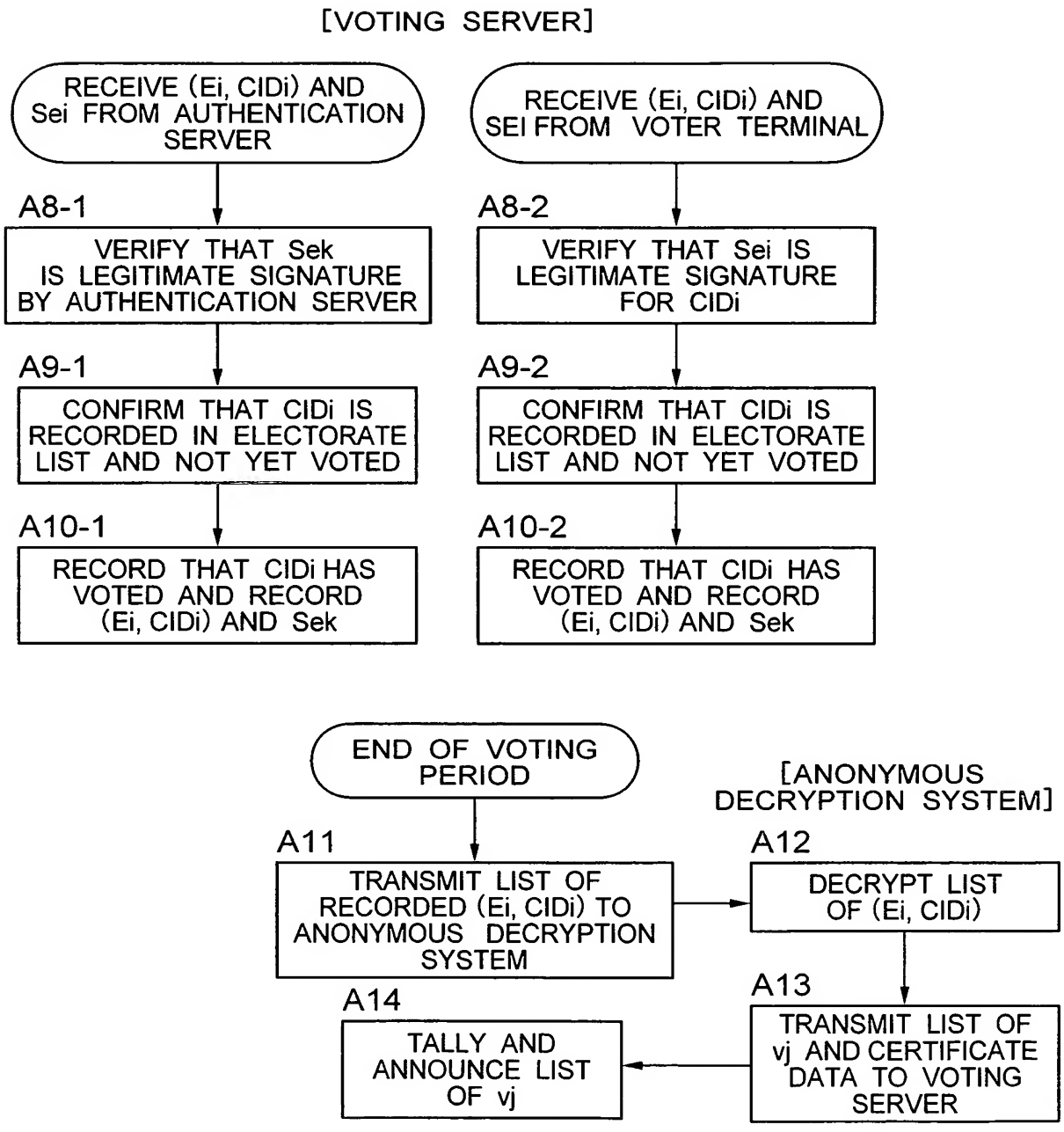

[VOTING SERVER]
RECEIVE (Ei, CIDi) AND Sei FROM AUTHENTICATION SERVER
RECEIVE (Ei, CIDi) AND SEI FROM VOTER TERMINAL
A8-1
VERIFY THAT Sek IS LEGITIMATE SIGNATURE BY AUTHENTICATION SERVER
A8-2
VERIFY THAT Sei IS LEGITIMATE SIGNATURE FOR CIDi
A9-1
CONFIRM THAT CIDi IS RECORDED IN ELECTORATE LIST AND NOT YET VOTED
A9-2
CONFIRM THAT CIDi IS RECORDED IN ELECTORATE LIST AND NOT YET VOTED
A10-1
RECORD THAT CIDi HAS VOTED AND RECORD (Ei, CIDi) AND Sek
A10-2
RECORD THAT CIDi HAS VOTED AND RECORD (Ei, CIDi) AND Sek
END OF VOTING PERIOD
[ANONYMOUS DECRYPTION SYSTEM]
A11
TRANSMIT LIST OF RECORDED (Ei, CIDi) TO ANONYMOUS DECRYPTION SYSTEM
A12
DECRYPT LIST OF (Ei, CIDi)
A13
TRANSMIT LIST OF vj AND CERTIFICATE DATA TO VOTING SERVER
A14
TALLY AND ANNOUNCE LIST OF vj

FIG.10

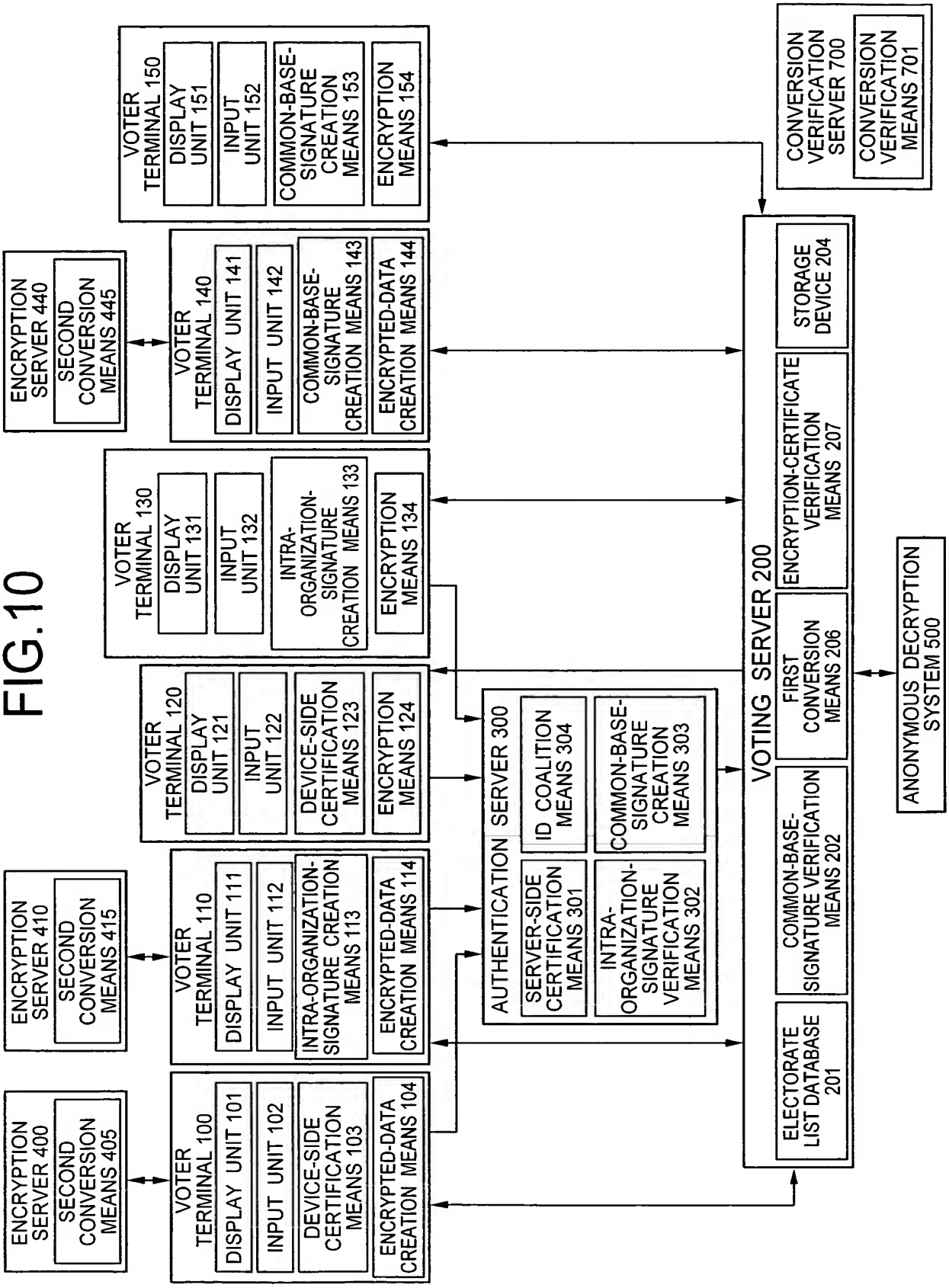

VOTER TERMINAL 150
DISPLAY UNIT 151
INPUT UNIT 152
COMMON-BASE-SIGNATURE CREATION MEANS 153
ENCRYPTION MEANS 154
ENCRYPTION SERVER 440
SECOND CONVERSION MEANS 445
VOTER TERMINAL 140
DISPLAY UNIT 141
INPUT UNIT 142
COMMON-BASE-SIGNATURE CREATION MEANS 143
ENCRYPTED-DATA CREATION MEANS 144
VOTER TERMINAL 130
DISPLAY UNIT 131
INPUT UNIT 132
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 133
ENCRYPTION MEANS 134
VOTER TERMINAL 120
DISPLAY UNIT 121
INPUT UNIT 122
DEVICE-SIDE CERTIFICATION MEANS 123
ENCRYPTION MEANS 124
ENCRYPTION SERVER 410
SECOND CONVERSION MEANS 415
VOTER TERMINAL 110
DISPLAY UNIT 111
INPUT UNIT 112
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 113
ENCRYPTED-DATA CREATION MEANS 114
ENCRYPTION SERVER 400
SECOND CONVERSION MEANS 405
VOTER TERMINAL 100
DISPLAY UNIT 101
INPUT UNIT 102
DEVICE-SIDE CERTIFICATION MEANS 103
ENCRYPTED-DATA CREATION MEANS 104
AUTHENTICATION SERVER 300
SERVER-SIDE CERTIFICATION MEANS 301
INTRA-ORGANIZATION-SIGNATURE VERIFICATION MEANS 302
ID COALITION MEANS 304
COMMON-BASE-SIGNATURE CREATION MEANS 303
VOTING SERVER 200
ELECTORATE LIST DATABASE 201
COMMON-BASE-SIGNATURE VERIFICATION MEANS 202
FIRST CONVERSION MEANS 206
ENCRYPTION-CERTIFICATE VERIFICATION MEANS 207
STORAGE DEVICE 204
CONVERSION VERIFICATION SERVER 700
CONVERSION VERIFICATION MEANS 701
ANONYMOUS DECRYPTION SYSTEM 500

FIG.11

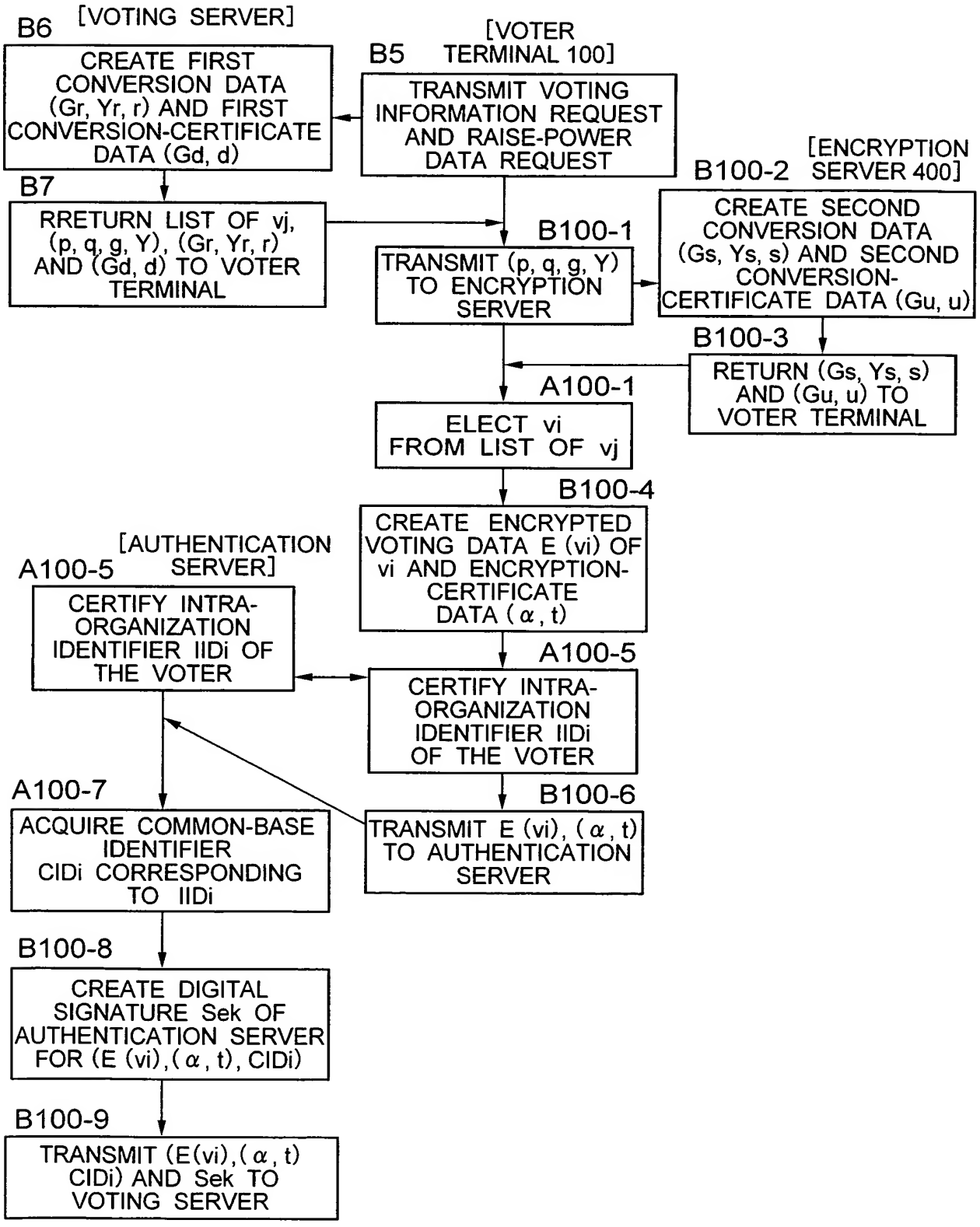

B6 [VOTING SERVER]
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
B5 [VOTER TERMINAL 100]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B100-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER
B100-2 [ENCRYPTION SERVER 400]
CREATE SECOND CONVERSION DATA (Gs, Ys, s) AND SECOND CONVERSION-CERTIFICATE DATA (Gu, u)
B100-3
RETURN (Gs, Ys, s) AND (Gu, u) TO VOTER TERMINAL
A100-1
ELECT vi FROM LIST OF vj
B100-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
A100-5 [AUTHENTICATION SERVER]
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
B100-6
TRANSMIT E (vi), (α, t) TO AUTHENTICATION SERVER
A100-7
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
B100-8
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E (vi), (α, t), CIDi)
B100-9
TRANSMIT (E(vi), (α, t) CIDi) AND Sek TO VOTING SERVER

FIG.12

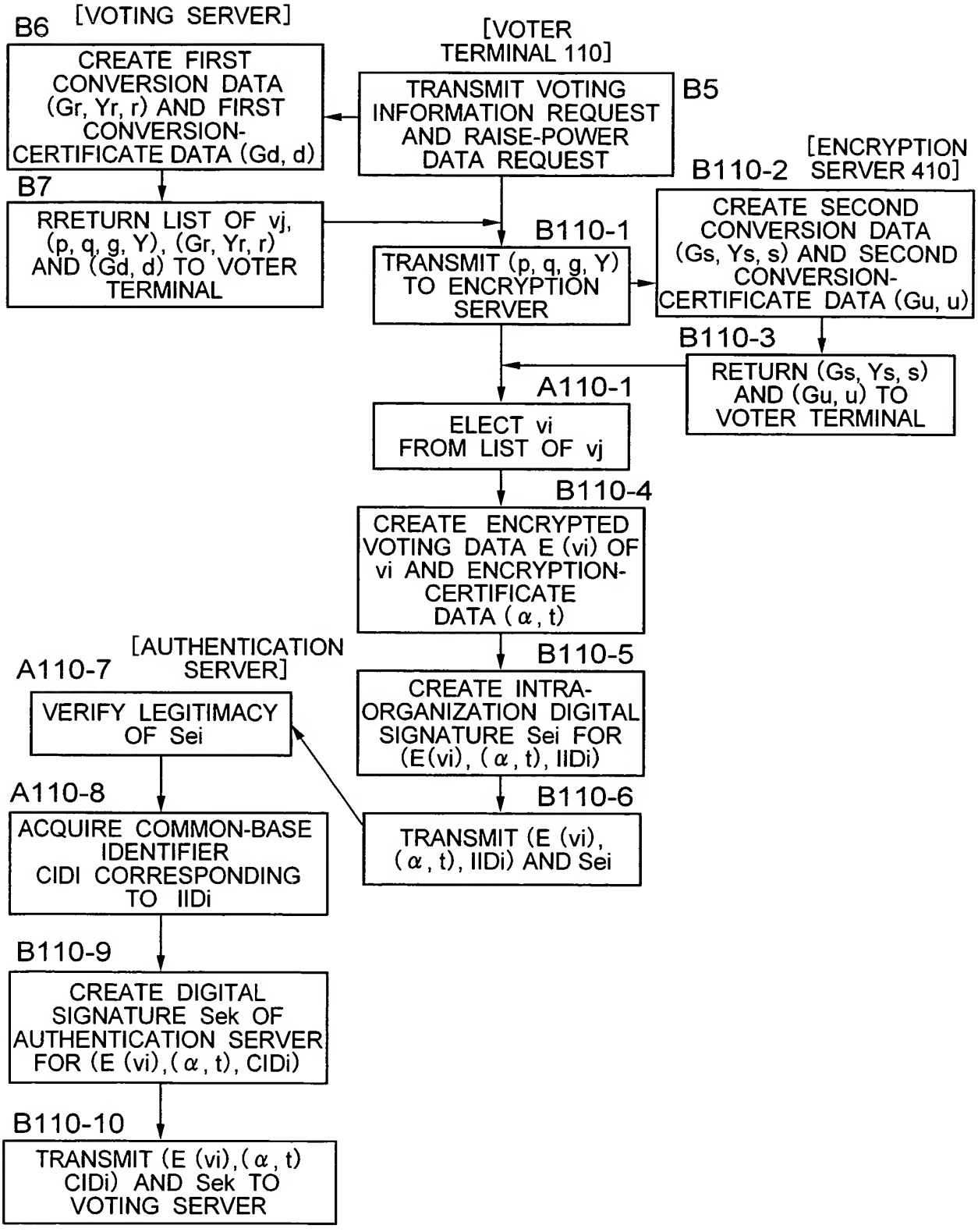

[VOTING SERVER]
B6
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
[VOTER TERMINAL 110]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B5
B110-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 410]
B110-2
CREATE SECOND CONVERSION DATA (Gs, Ys, s) AND SECOND CONVERSION-CERTIFICATE DATA (Gu, u)
B110-3
RETURN (Gs, Ys, s) AND (Gu, u) TO VOTER TERMINAL
A110-1
ELECT vi FROM LIST OF vj
B110-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
B110-5
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E(vi), (α, t), IIDi)
B110-6
TRANSMIT (E (vi), (α, t), IIDi) AND Sei
[AUTHENTICATION SERVER]
A110-7
VERIFY LEGITIMACY OF Sei
A110-8
ACQUIRE COMMON-BASE IDENTIFIER CIDI CORRESPONDING TO IIDi
B110-9
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E (vi), (α, t), CIDi)
B110-10
TRANSMIT (E (vi), (α, t) CIDi) AND Sek TO VOTING SERVER

FIG.13

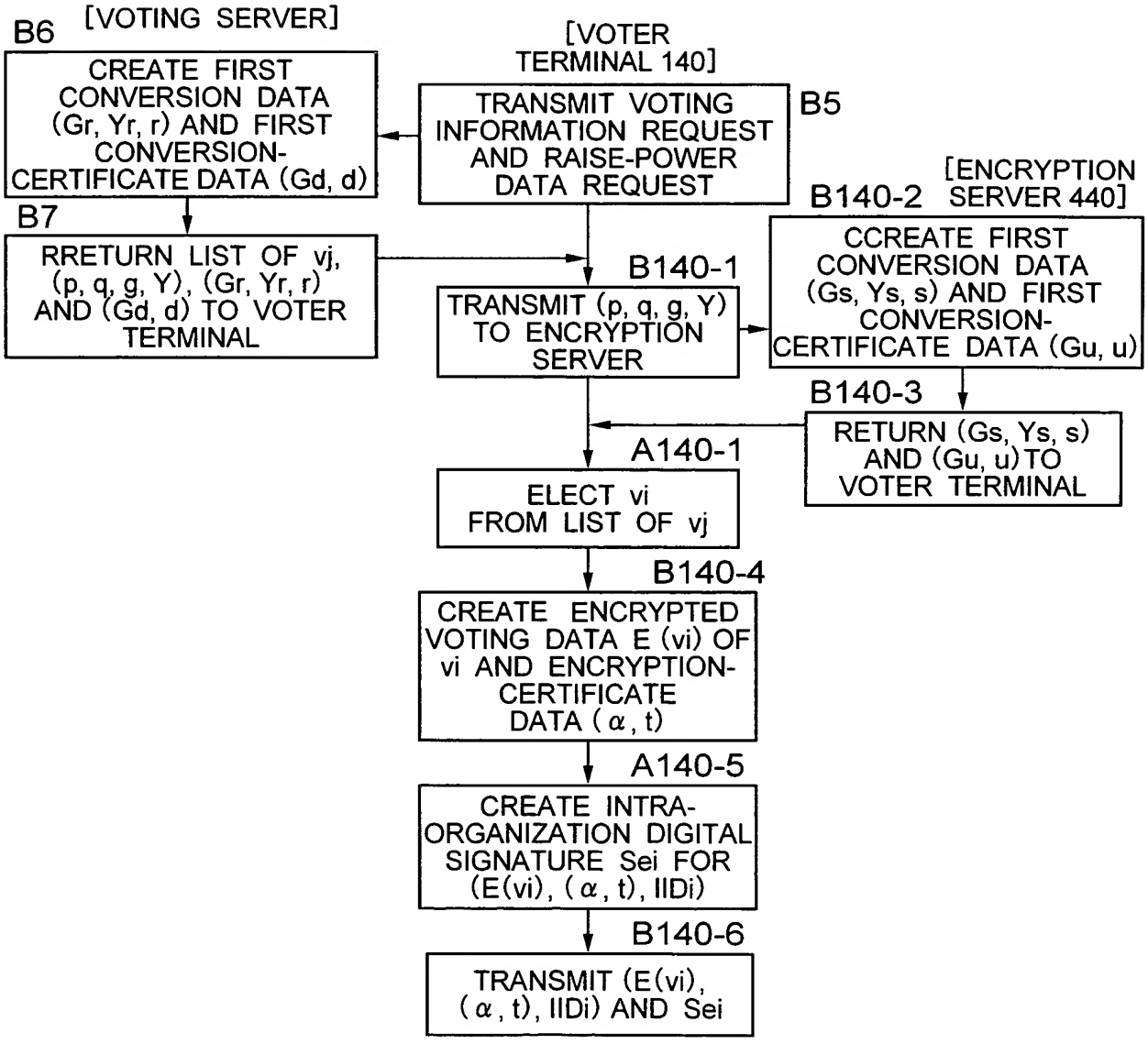

B6
[VOTING SERVER]
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
[VOTER TERMINAL 140]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B5
B140-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER
B140-2
[ENCRYPTION SERVER 440]
CCREATE FIRST CONVERSION DATA (Gs, Ys, s) AND FIRST CONVERSION-CERTIFICATE DATA (Gu, u)
B140-3
RETURN (Gs, Ys, s) AND (Gu, u) TO VOTER TERMINAL
A140-1
ELECT vi FROM LIST OF vj
B140-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
A140-5
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E(vi), (α, t), IIDi)
B140-6
TRANSMIT (E(vi), (α, t), IIDi) AND Sei

FIG.14

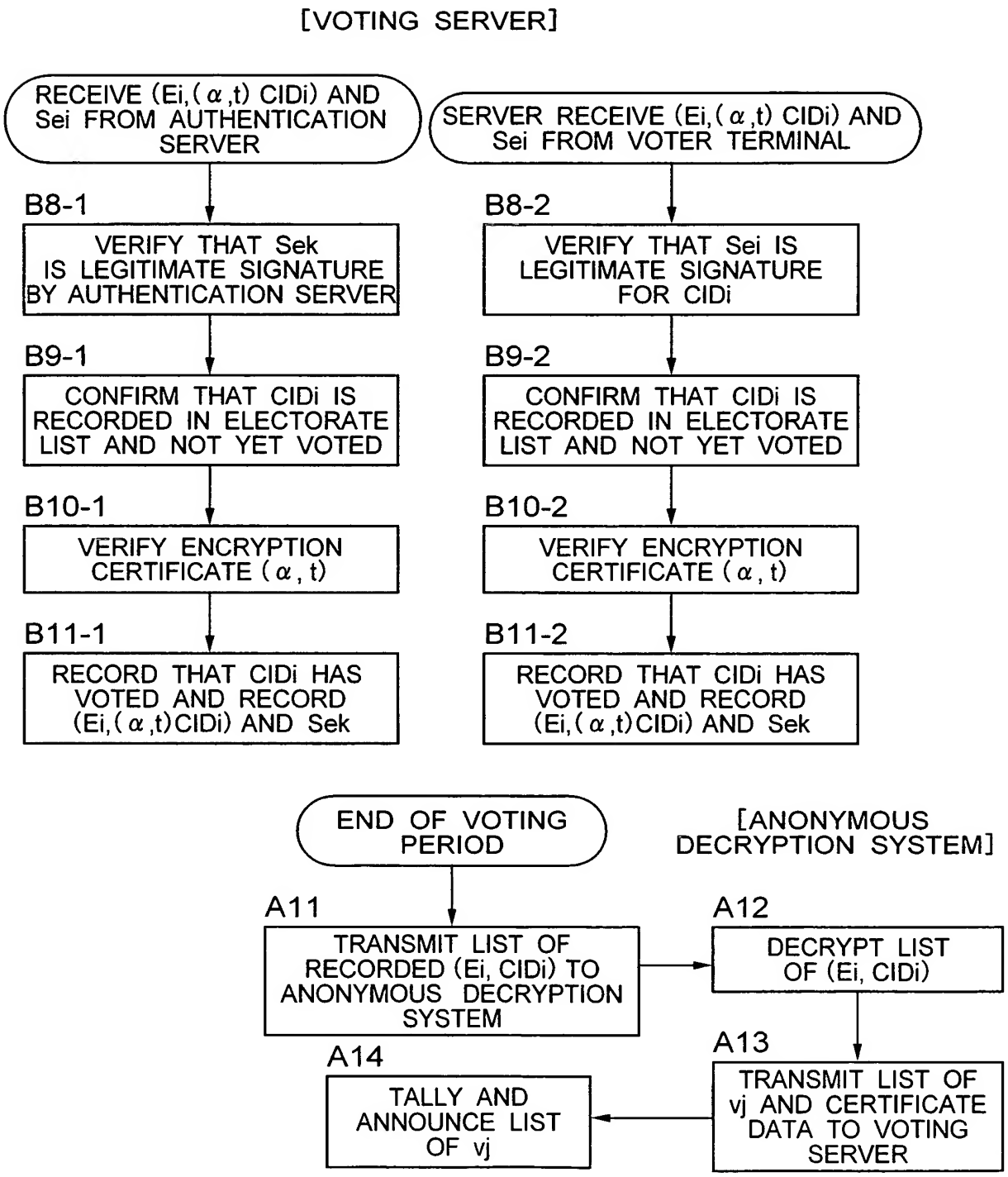

[VOTING SERVER]
RECEIVE (Ei,(α,t) CIDi) AND Sei FROM AUTHENTICATION SERVER
SERVER RECEIVE (Ei,(α,t) CIDi) AND Sei FROM VOTER TERMINAL
B8-1
VERIFY THAT Sek IS LEGITIMATE SIGNATURE BY AUTHENTICATION SERVER
B8-2
VERIFY THAT Sei IS LEGITIMATE SIGNATURE FOR CIDi
B9-1
CONFIRM THAT CIDi IS RECORDED IN ELECTORATE LIST AND NOT YET VOTED
B9-2
CONFIRM THAT CIDi IS RECORDED IN ELECTORATE LIST AND NOT YET VOTED
B10-1
VERIFY ENCRYPTION CERTIFICATE (α, t)
B10-2
VERIFY ENCRYPTION CERTIFICATE (α, t)
B11-1
RECORD THAT CIDi HAS VOTED AND RECORD (Ei,(α,t)CIDi) AND Sek
B11-2
RECORD THAT CIDi HAS VOTED AND RECORD (Ei,(α,t)CIDi) AND Sek
END OF VOTING PERIOD
[ANONYMOUS DECRYPTION SYSTEM]
A11
TRANSMIT LIST OF RECORDED (Ei, CIDi) TO ANONYMOUS DECRYPTION SYSTEM
A12
DECRYPT LIST OF (Ei, CIDi)
A13
TRANSMIT LIST OF vj AND CERTIFICATE DATA TO VOTING SERVER
A14
TALLY AND ANNOUNCE LIST OF vj

FIG.15

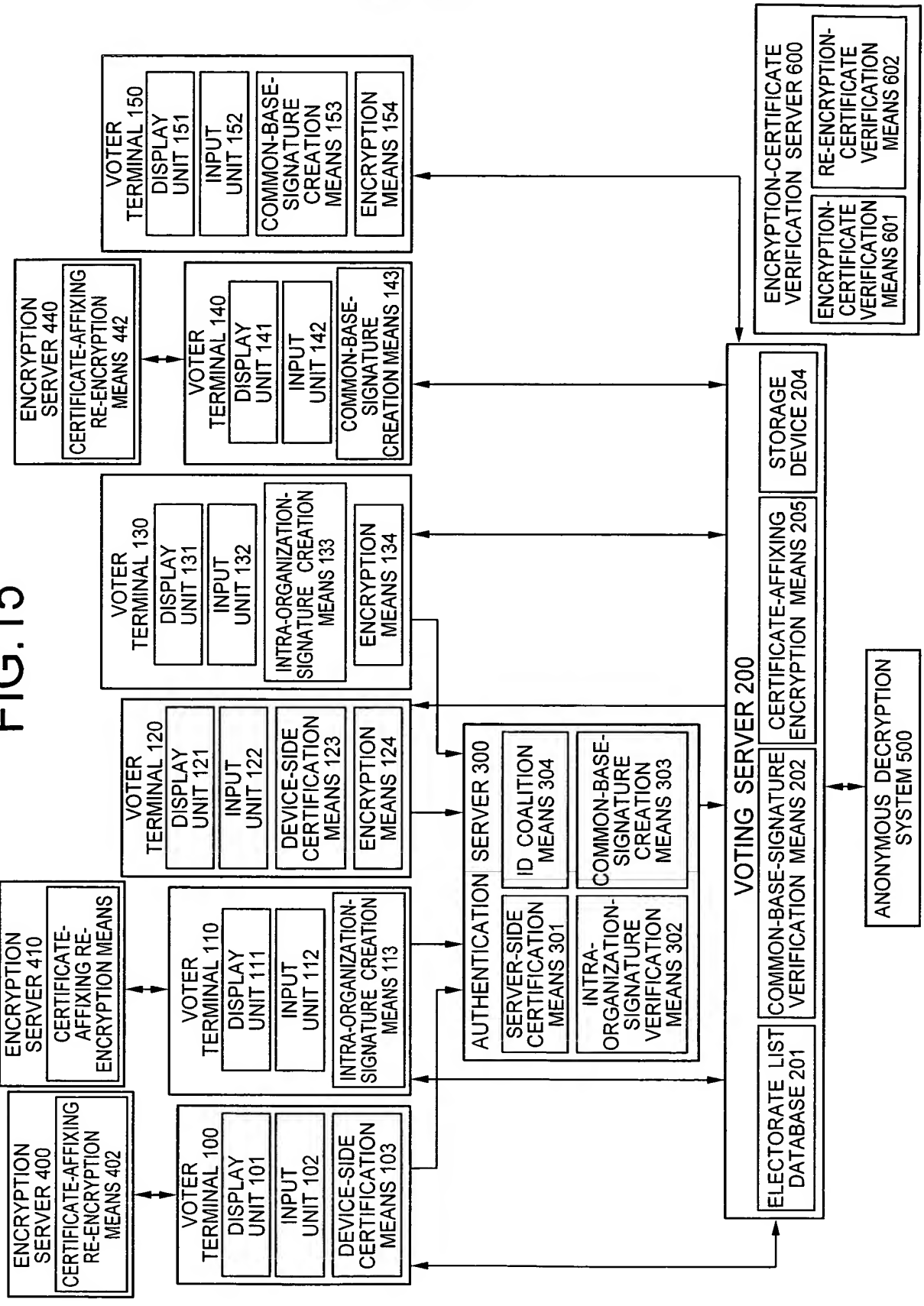

VOTER TERMINAL 150
DISPLAY UNIT 151
INPUT UNIT 152
COMMON-BASE-SIGNATURE CREATION MEANS 153
ENCRYPTION MEANS 154
ENCRYPTION SERVER 440
CERTIFICATE-AFFIXING RE-ENCRYPTION MEANS 442
VOTER TERMINAL 140
DISPLAY UNIT 141
INPUT UNIT 142
COMMON-BASE-SIGNATURE CREATION MEANS 143
VOTER TERMINAL 130
DISPLAY UNIT 131
INPUT UNIT 132
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 133
ENCRYPTION MEANS 134
VOTER TERMINAL 120
DISPLAY UNIT 121
INPUT UNIT 122
DEVICE-SIDE CERTIFICATION MEANS 123
ENCRYPTION MEANS 124
ENCRYPTION SERVER 410
CERTIFICATE-AFFIXING RE-ENCRYPTION MEANS
VOTER TERMINAL 110
DISPLAY UNIT 111
INPUT UNIT 112
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 113
ENCRYPTION SERVER 400
CERTIFICATE-AFFIXING RE-ENCRYPTION MEANS 402
VOTER TERMINAL 100
DISPLAY UNIT 101
INPUT UNIT 102
DEVICE-SIDE CERTIFICATION MEANS 103
AUTHENTICATION SERVER 300
SERVER-SIDE CERTIFICATION MEANS 301
ID COALITION MEANS 304
INTRA-ORGANIZATION-SIGNATURE VERIFICATION MEANS 302
COMMON-BASE-SIGNATURE CREATION MEANS 303
VOTING SERVER 200
ELECTORATE LIST DATABASE 201
COMMON-BASE-SIGNATURE VERIFICATION MEANS 202
CERTIFICATE-AFFIXING ENCRYPTION MEANS 205
STORAGE DEVICE 204
ENCRYPTION-CERTIFICATE VERIFICATION SERVER 600
ENCRYPTION-CERTIFICATE VERIFICATION MEANS 601
RE-ENCRYPTION-CERTIFICATE VERIFICATION MEANS 602
ANONYMOUS DECRYPTION SYSTEM 500

FIG.16

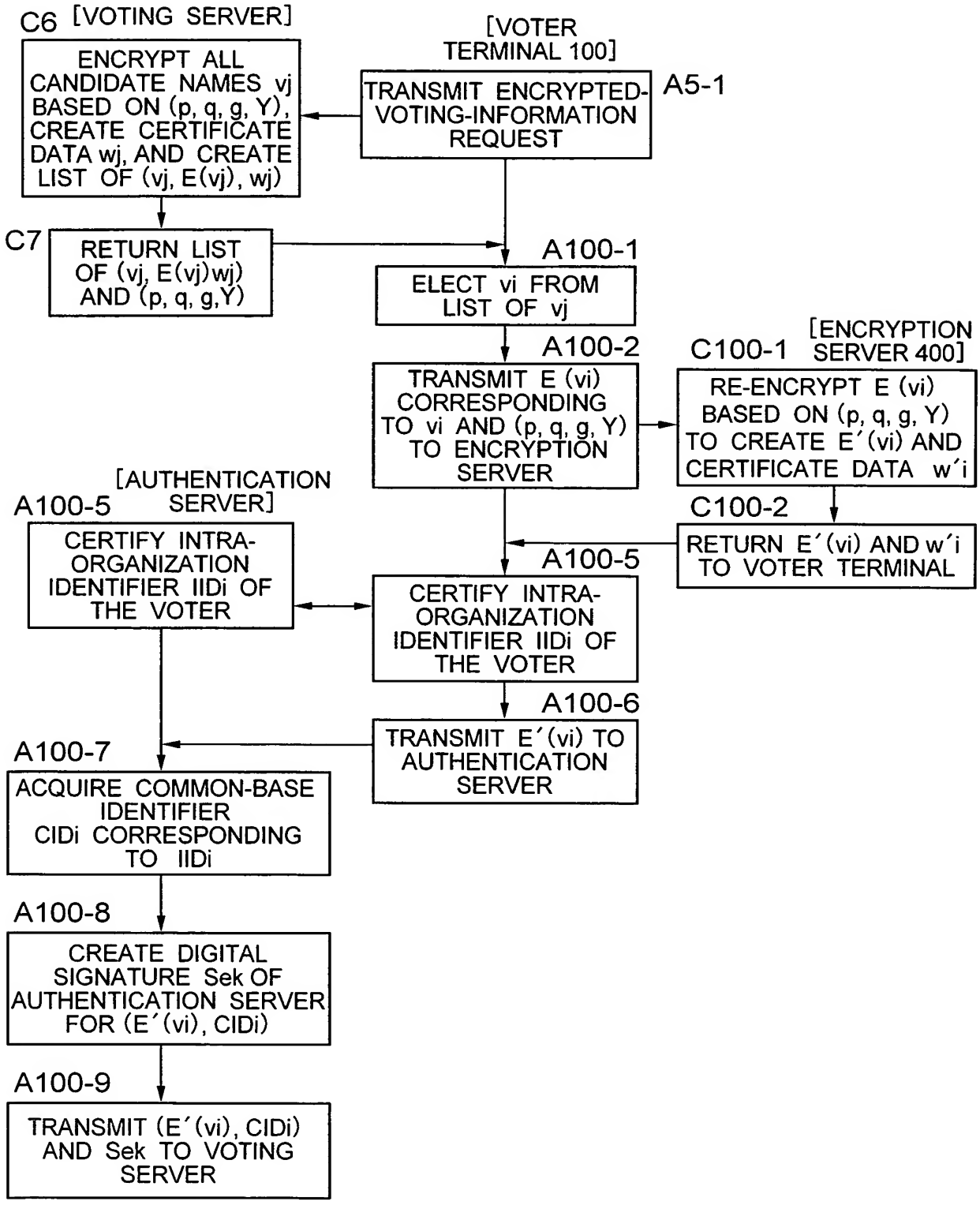

C6 [VOTING SERVER]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y), CREATE CERTIFICATE DATA wj, AND CREATE LIST OF (vj, E(vj), wj)
[VOTER TERMINAL 100]
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
C7
RETURN LIST OF (vj, E(vj)wj) AND (p, q, g,Y)
A100-1
ELECT vi FROM LIST OF vj
A100-2
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
C100-1 [ENCRYPTION SERVER 400]
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CREATE E'(vi) AND CERTIFICATE DATA w'i
C100-2
RETURN E'(vi) AND w'i TO VOTER TERMINAL
[AUTHENTICATION SERVER]
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-6
TRANSMIT E'(vi) TO AUTHENTICATION SERVER
A100-7
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A100-8
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E'(vi), CIDi)
A100-9
TRANSMIT (E'(vi), CIDi) AND Sek TO VOTING SERVER

FIG.17

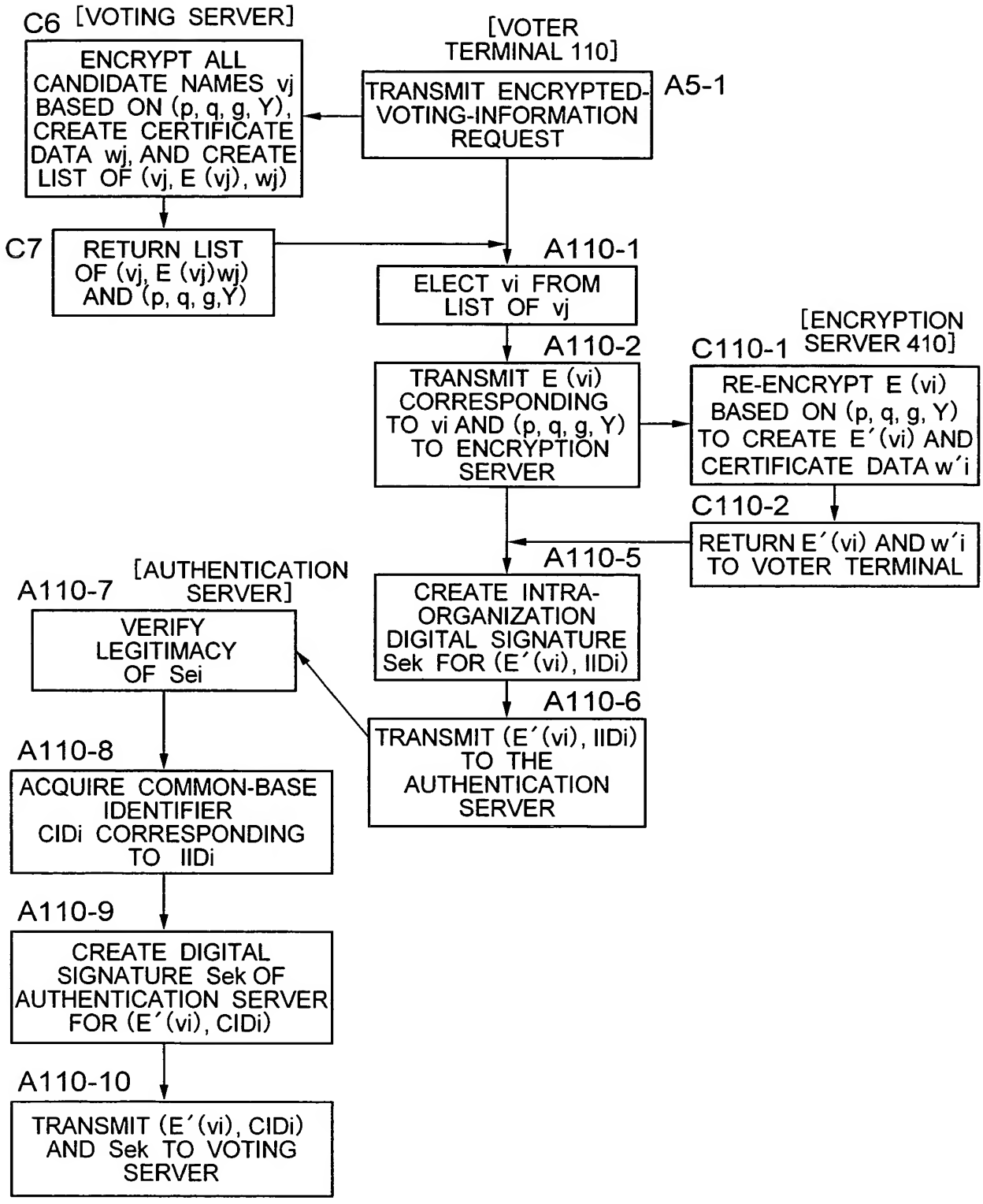

C6 [VOTING SERVER]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y), CREATE CERTIFICATE DATA wj, AND CREATE LIST OF (vj, E (vj), wj)
[VOTER TERMINAL 110]
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
C7
RETURN LIST OF (vj, E (vj)wj) AND (p, q, g,Y)
A110-1
ELECT vi FROM LIST OF vj
A110-2
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 410]
C110-1
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CREATE E′(vi) AND CERTIFICATE DATA w′i
C110-2
RETURN E′(vi) AND w′i TO VOTER TERMINAL
A110-5
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sek FOR (E′(vi), IIDi)
A110-6
TRANSMIT (E′(vi), IIDi) TO THE AUTHENTICATION SERVER
[AUTHENTICATION SERVER]
A110-7
VERIFY LEGITIMACY OF Sei
A110-8
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
A110-9
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E′(vi), CIDi)
A110-10
TRANSMIT (E′(vi), CIDi) AND Sek TO VOTING SERVER

FIG.18

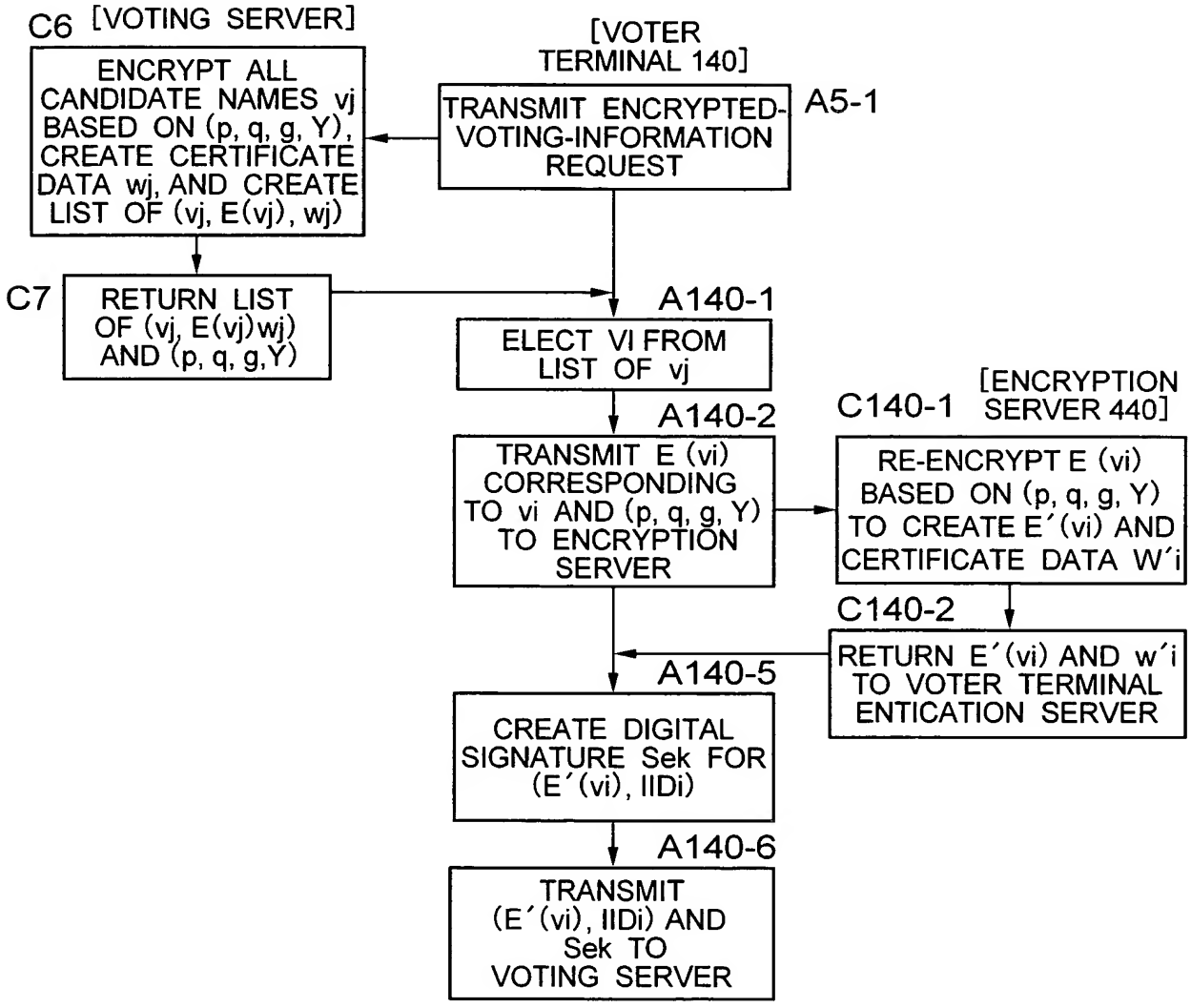

C6 [VOTING SERVER]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y), CREATE CERTIFICATE DATA wj, AND CREATE LIST OF (vj, E(vj), wj)
C7
RETURN LIST OF (vj, E(vj)wj) AND (p, q, g,Y)
[VOTER TERMINAL 140]
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
A140-1
ELECT VI FROM LIST OF vj
A140-2
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
C140-1 [ENCRYPTION SERVER 440]
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CREATE E′(vi) AND CERTIFICATE DATA W′i
C140-2
RETURN E′(vi) AND w′i TO VOTER TERMINAL ENTICATION SERVER
A140-5
CREATE DIGITAL SIGNATURE Sek FOR (E′(vi), IIDi)
A140-6
TRANSMIT (E′(vi), IIDi) AND Sek TO VOTING SERVER

FIG.19

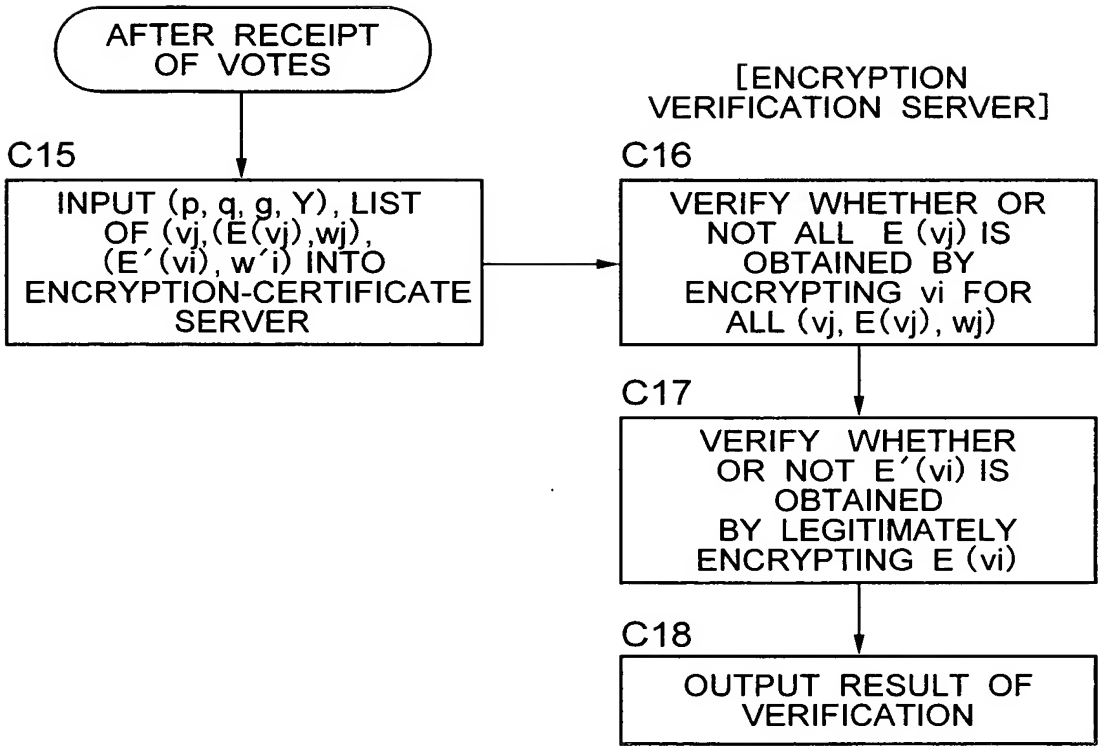

AFTER RECEIPT OF VOTES
[ENCRYPTION VERIFICATION SERVER]
C15
INPUT (p, q, g, Y), LIST OF (vj,(E(vj),wj), (E´(vi), w´i) INTO ENCRYPTION-CERTIFICATE SERVER
C16
VERIFY WHETHER OR NOT ALL E (vj) IS OBTAINED BY ENCRYPTING vi FOR ALL (vj, E(vj), wj)
C17
VERIFY WHETHER OR NOT E´(vi) IS OBTAINED BY LEGITIMATELY ENCRYPTING E (vi)
C18
OUTPUT RESULT OF VERIFICATION

FIG.20

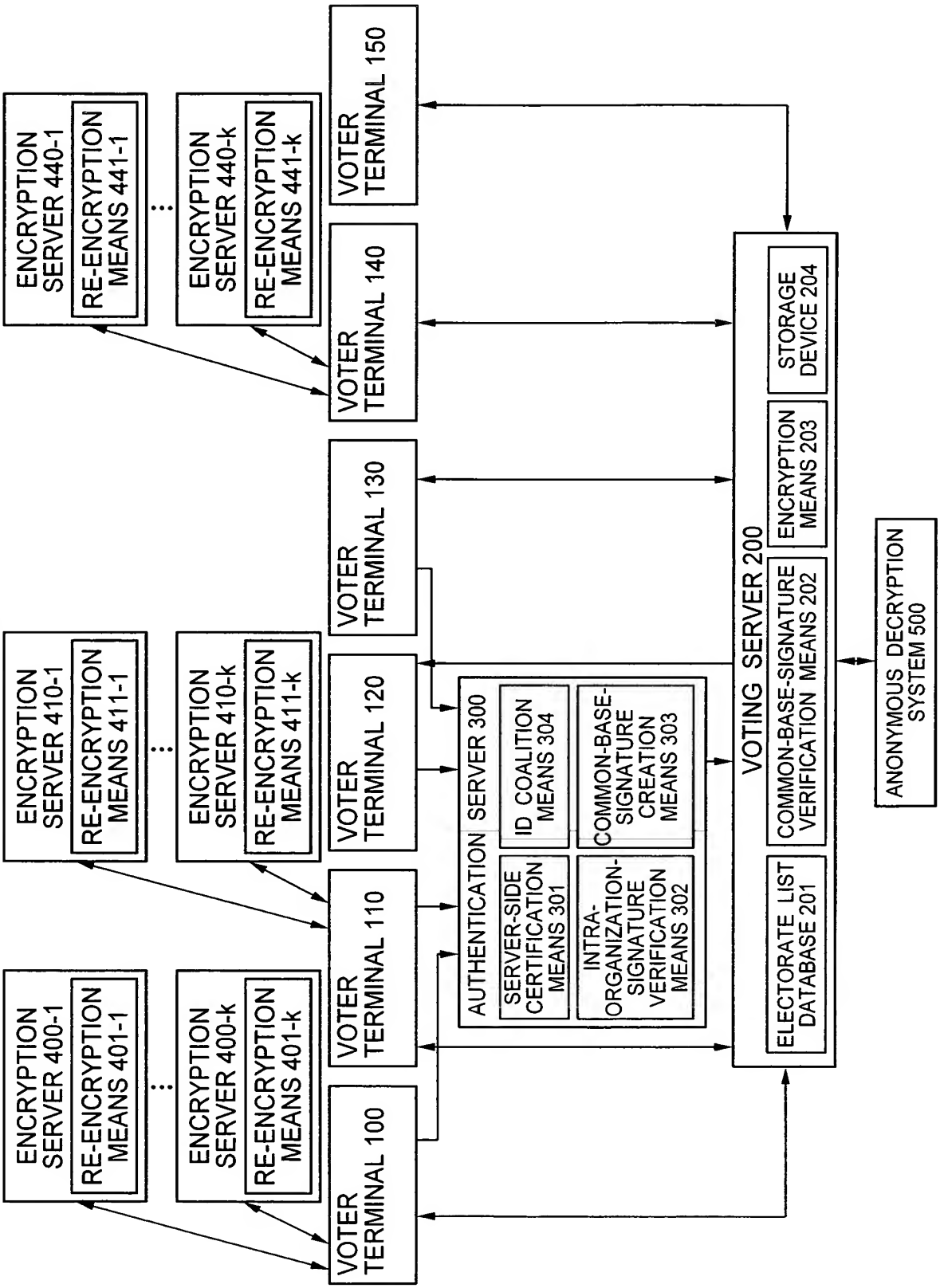

ENCRYPTION SERVER 400-1
RE-ENCRYPTION MEANS 401-1
ENCRYPTION SERVER 400-k
RE-ENCRYPTION MEANS 401-k
ENCRYPTION SERVER 410-1
RE-ENCRYPTION MEANS 411-1
ENCRYPTION SERVER 410-k
RE-ENCRYPTION MEANS 411-k
ENCRYPTION SERVER 440-1
RE-ENCRYPTION MEANS 441-1
ENCRYPTION SERVER 440-k
RE-ENCRYPTION MEANS 441-k
VOTER TERMINAL 100
VOTER TERMINAL 110
VOTER TERMINAL 120
VOTER TERMINAL 130
VOTER TERMINAL 140
VOTER TERMINAL 150
AUTHENTICATION SERVER 300
SERVER-SIDE CERTIFICATION MEANS 301
INTRA-ORGANIZATION-SIGNATURE VERIFICATION MEANS 302
ID COALITION MEANS 304
COMMON-BASE-SIGNATURE CREATION MEANS 303
VOTING SERVER 200
ELECTORATE LIST DATABASE 201
COMMON-BASE-SIGNATURE VERIFICATION MEANS 202
ENCRYPTION MEANS 203
STORAGE DEVICE 204
ANONYMOUS DECRYPTION SYSTEM 500

FIG.21

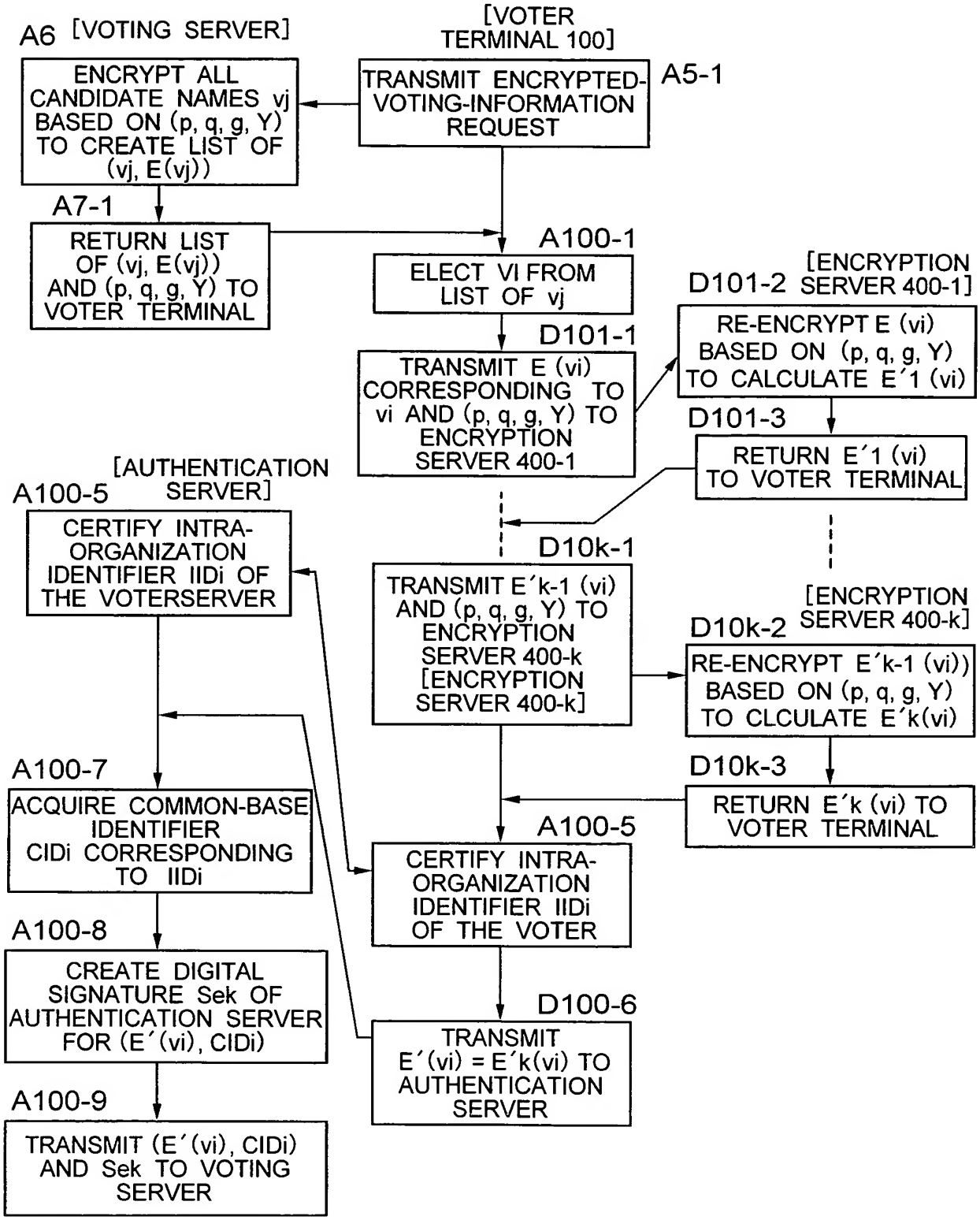

A6 [VOTING SERVER]
[VOTER TERMINAL 100]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
A7-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y) TO VOTER TERMINAL
A100-1
ELECT VI FROM LIST OF vj
D101-1
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER 400-1
[ENCRYPTION SERVER 400-1]
D101-2
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E'1 (vi)
D101-3
RETURN E'1 (vi) TO VOTER TERMINAL
[AUTHENTICATION SERVER]
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTERSERVER
D10k-1
TRANSMIT E'k-1 (vi) AND (p, q, g, Y) TO ENCRYPTION SERVER 400-k [ENCRYPTION SERVER 400-k]
[ENCRYPTION SERVER 400-k]
D10k-2
RE-ENCRYPT E'k-1 (vi)) BASED ON (p, q, g, Y) TO CLCULATE E'k(vi)
A100-7
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
D10k-3
RETURN E'k (vi) TO VOTER TERMINAL
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
A100-8
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E'(vi), CIDi)
D100-6
TRANSMIT E'(vi) = E'k(vi) TO AUTHENTICATION SERVER
A100-9
TRANSMIT (E'(vi), CIDi) AND Sek TO VOTING SERVER

FIG.22

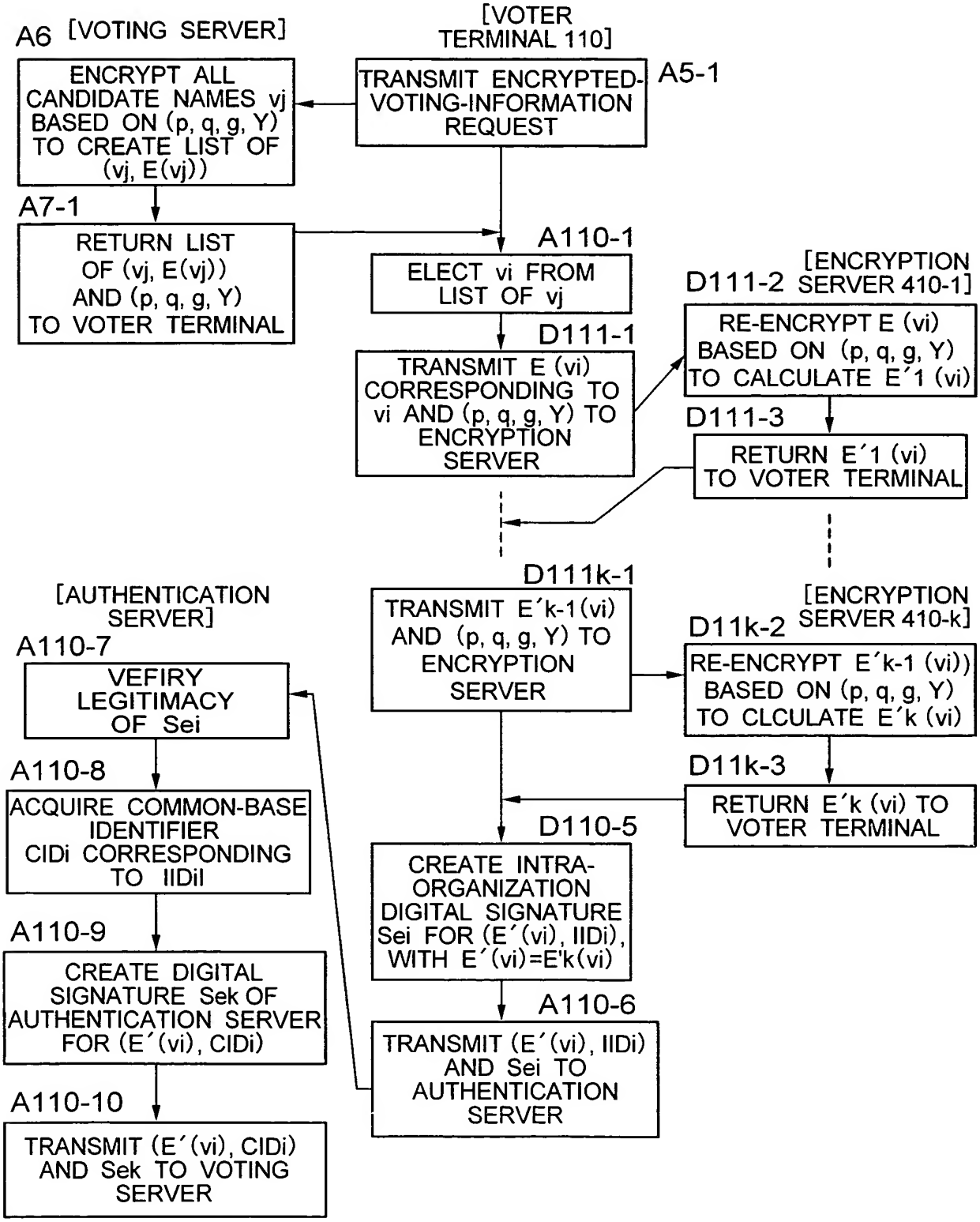

A6 [VOTING SERVER]
[VOTER TERMINAL 110]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A5-1
A7-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y) TO VOTER TERMINAL
A110-1
ELECT vi FROM LIST OF vj
D111-1
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 410-1]
D111-2
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E'1 (vi)
D111-3
RETURN E'1 (vi) TO VOTER TERMINAL
D111k-1
TRANSMIT E'k-1(vi) AND (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 410-k]
D11k-2
RE-ENCRYPT E'k-1 (vi)) BASED ON (p, q, g, Y) TO CLCULATE E'k (vi)
D11k-3
RETURN E'k (vi) TO VOTER TERMINAL
[AUTHENTICATION SERVER]
A110-7
VEFIRY LEGITIMACY OF Sei
A110-8
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDiI
A110-9
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E'(vi), CIDi)
A110-10
TRANSMIT (E'(vi), CIDi) AND Sek TO VOTING SERVER
D110-5
CREATE INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E'(vi), IIDi), WITH E'(vi)=E'k(vi)
A110-6
TRANSMIT (E'(vi), IIDi) AND Sei TO AUTHENTICATION SERVER

FIG.23

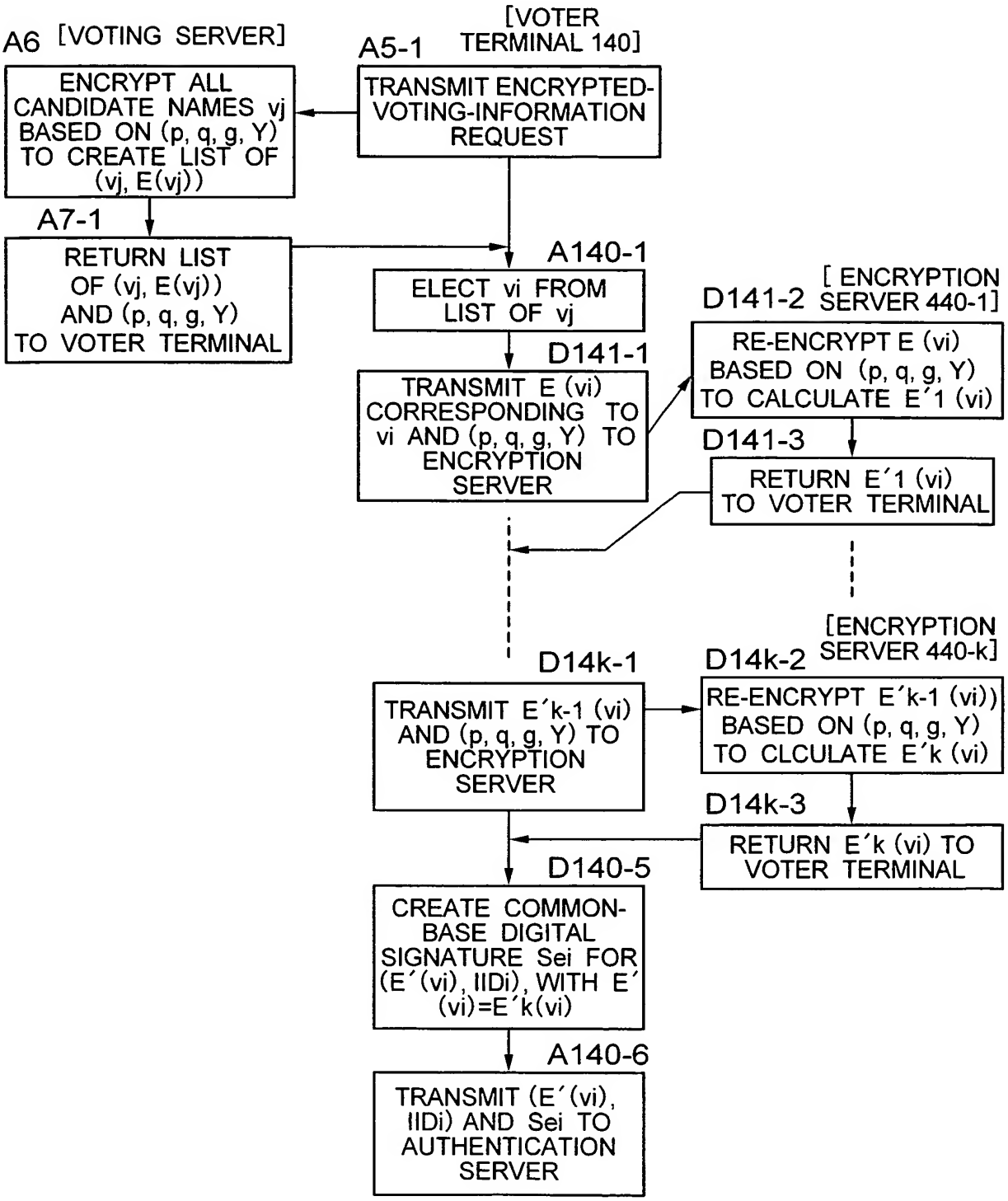

A6 [VOTING SERVER]
ENCRYPT ALL CANDIDATE NAMES vj BASED ON (p, q, g, Y) TO CREATE LIST OF (vj, E(vj))
A7-1
RETURN LIST OF (vj, E(vj)) AND (p, q, g, Y) TO VOTER TERMINAL
[VOTER TERMINAL 140]
A5-1
TRANSMIT ENCRYPTED-VOTING-INFORMATION REQUEST
A140-1
ELECT vi FROM LIST OF vj
D141-1
TRANSMIT E (vi) CORRESPONDING TO vi AND (p, q, g, Y) TO ENCRYPTION SERVER
[ENCRYPTION SERVER 440-1]
D141-2
RE-ENCRYPT E (vi) BASED ON (p, q, g, Y) TO CALCULATE E'1 (vi)
D141-3
RETURN E'1 (vi) TO VOTER TERMINAL
[ENCRYPTION SERVER 440-k]
D14k-1
TRANSMIT E'k-1 (vi) AND (p, q, g, Y) TO ENCRYPTION SERVER
D14k-2
RE-ENCRYPT E'k-1 (vi)) BASED ON (p, q, g, Y) TO CLCULATE E'k (vi)
D14k-3
RETURN E'k (vi) TO VOTER TERMINAL
D140-5
CREATE COMMON-BASE DIGITAL SIGNATURE Sei FOR (E'(vi), IIDi), WITH E'(vi)=E'k(vi)
A140-6
TRANSMIT (E'(vi), IIDi) AND Sei TO AUTHENTICATION SERVER

FIG.24

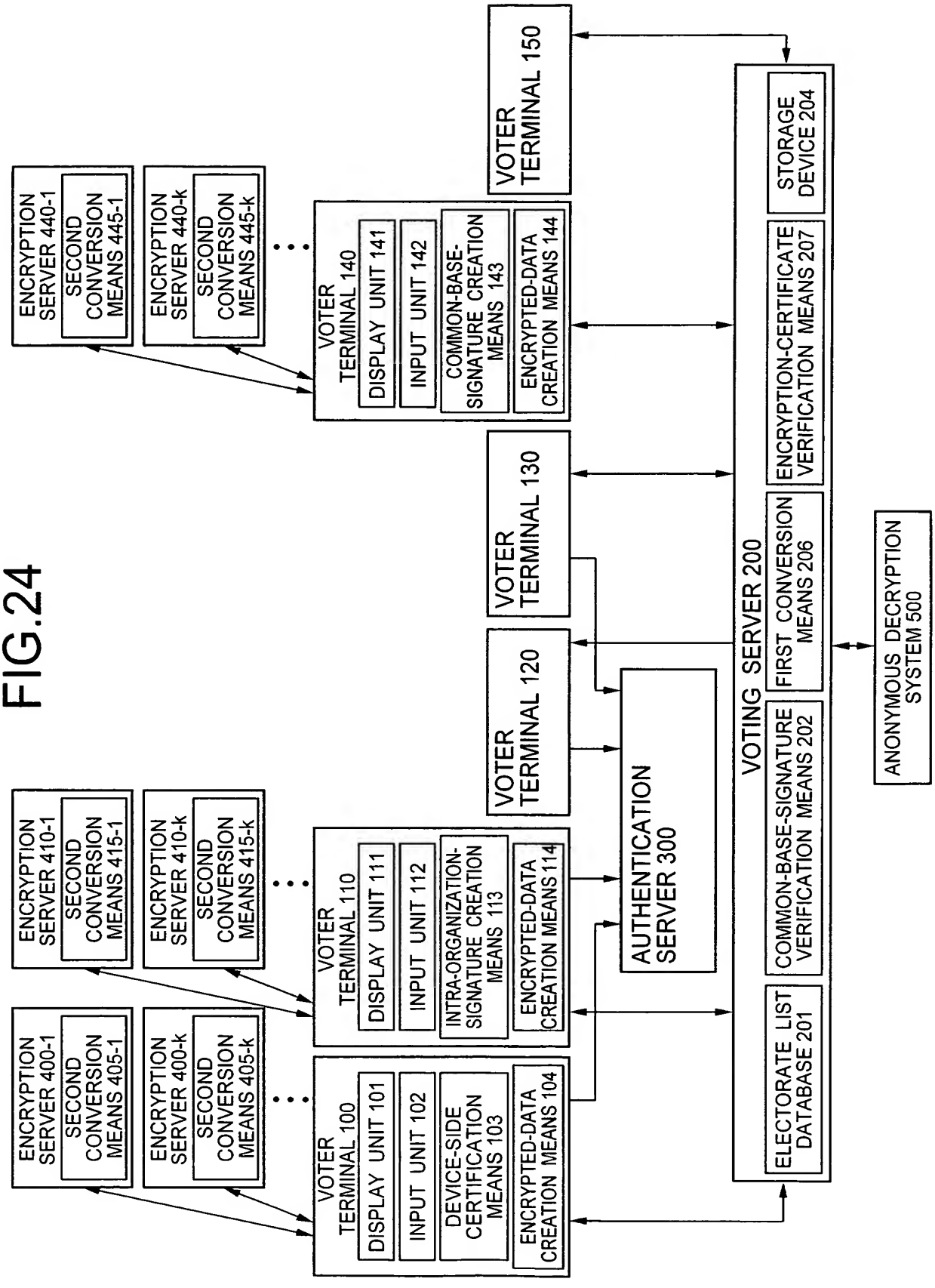

ENCRYPTION SERVER 400-1
SECOND CONVERSION MEANS 405-1
ENCRYPTION SERVER 400-k
SECOND CONVERSION MEANS 405-k
ENCRYPTION SERVER 410-1
SECOND CONVERSION MEANS 415-1
ENCRYPTION SERVER 410-k
SECOND CONVERSION MEANS 415-k
ENCRYPTION SERVER 440-1
SECOND CONVERSION MEANS 445-1
ENCRYPTION SERVER 440-k
SECOND CONVERSION MEANS 445-k
VOTER TERMINAL 100
DISPLAY UNIT 101
INPUT UNIT 102
DEVICE-SIDE CERTIFICATION MEANS 103
ENCRYPTED-DATA CREATION MEANS 104
VOTER TERMINAL 110
DISPLAY UNIT 111
INPUT UNIT 112
INTRA-ORGANIZATION-SIGNATURE CREATION MEANS 113
ENCRYPTED-DATA CREATION MEANS 114
VOTER TERMINAL 120
VOTER TERMINAL 130
VOTER TERMINAL 140
DISPLAY UNIT 141
INPUT UNIT 142
COMMON-BASE-SIGNATURE CREATION MEANS 143
ENCRYPTED-DATA CREATION MEANS 144
VOTER TERMINAL 150
AUTHENTICATION SERVER 300
VOTING SERVER 200
ELECTORATE LIST DATABASE 201
COMMON-BASE-SIGNATURE VERIFICATION MEANS 202
FIRST CONVERSION MEANS 206
ENCRYPTION-CERTIFICATE VERIFICATION MEANS 207
STORAGE DEVICE 204
ANONYMOUS DECRYPTION SYSTEM 500

FIG.25

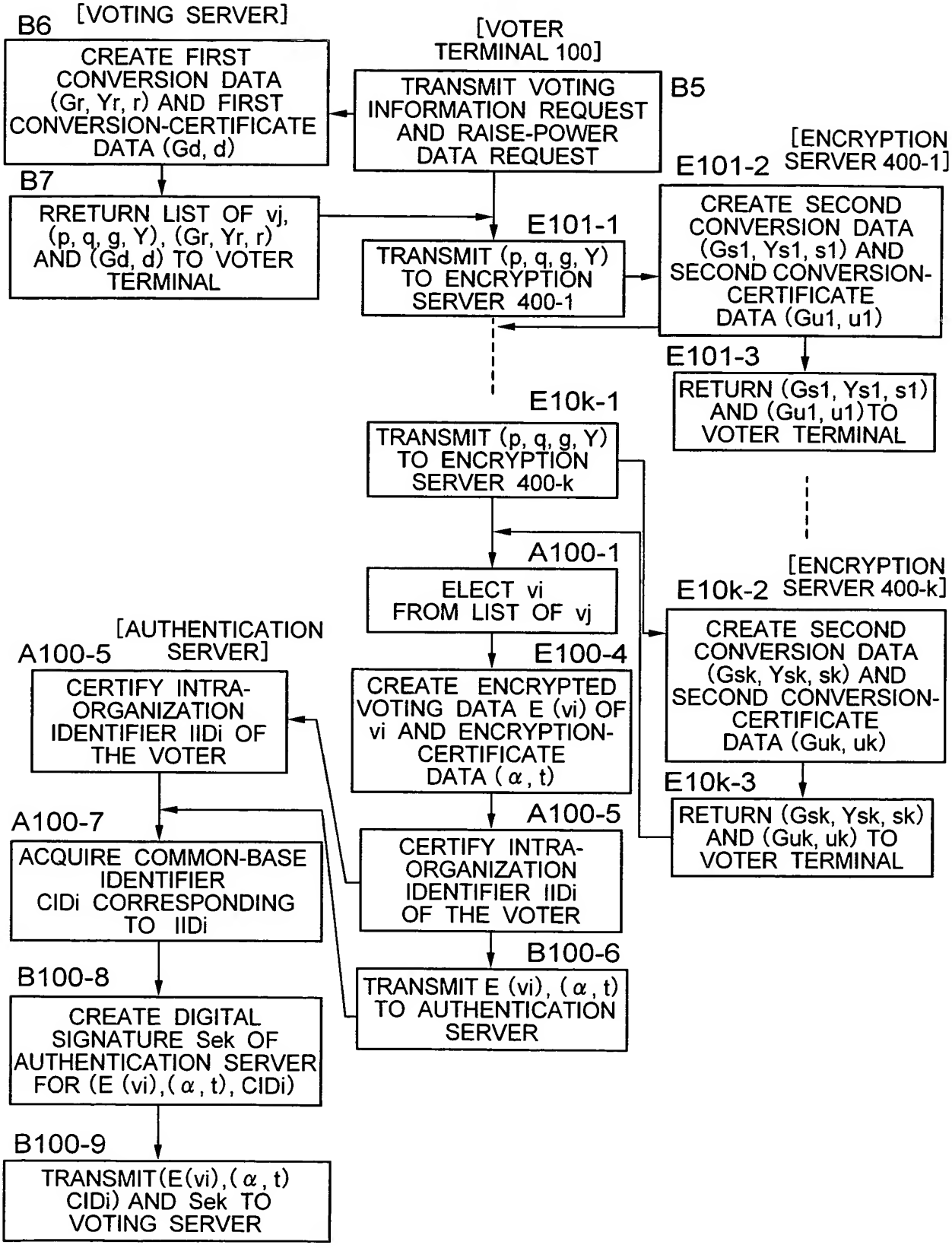

[VOTING SERVER]
B6
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
[VOTER TERMINAL 100]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B5
E101-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 400-1
[ENCRYPTION SERVER 400-1]
E101-2
CREATE SECOND CONVERSION DATA (Gs1, Ys1, s1) AND SECOND CONVERSION-CERTIFICATE DATA (Gu1, u1)
E101-3
RETURN (Gs1, Ys1, s1) AND (Gu1, u1) TO VOTER TERMINAL
E10k-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 400-k
A100-1
ELECT vi FROM LIST OF vj
[ENCRYPTION SERVER 400-k]
E10k-2
CREATE SECOND CONVERSION DATA (Gsk, Ysk, sk) AND SECOND CONVERSION-CERTIFICATE DATA (Guk, uk)
E10k-3
RETURN (Gsk, Ysk, sk) AND (Guk, uk) TO VOTER TERMINAL
[AUTHENTICATION SERVER]
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
E100-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
A100-5
CERTIFY INTRA-ORGANIZATION IDENTIFIER IIDi OF THE VOTER
B100-6
TRANSMIT E (vi), (α, t) TO AUTHENTICATION SERVER
A100-7
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
B100-8
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E (vi), (α, t), CIDi)
B100-9
TRANSMIT (E(vi), (α, t) CIDi) AND Sek TO VOTING SERVER

FIG.26

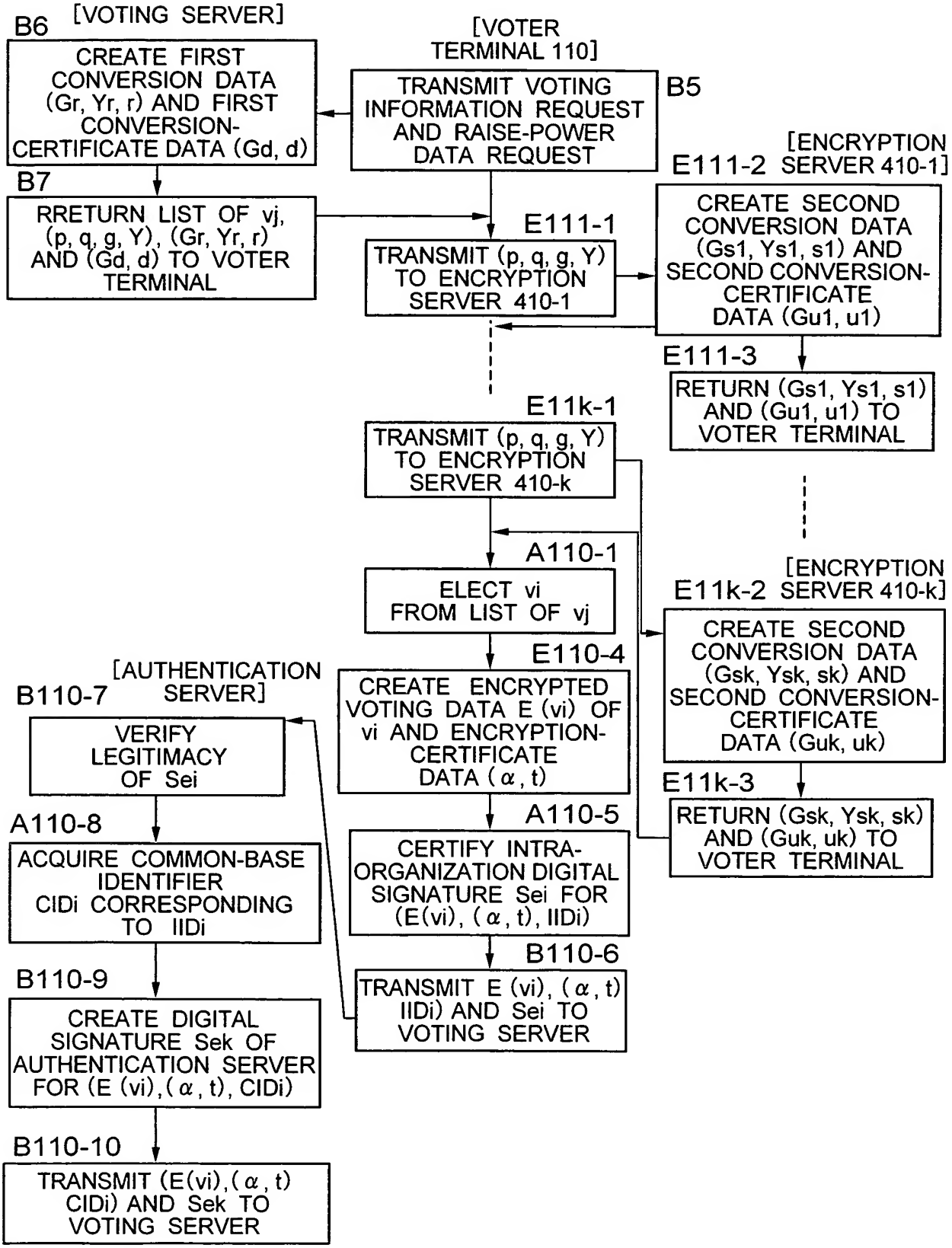

[VOTING SERVER]
B6
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
[VOTER TERMINAL 110]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B5
E111-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 410-1
[ENCRYPTION SERVER 410-1]
E111-2
CREATE SECOND CONVERSION DATA (Gs1, Ys1, s1) AND SECOND CONVERSION-CERTIFICATE DATA (Gu1, u1)
E111-3
RETURN (Gs1, Ys1, s1) AND (Gu1, u1) TO VOTER TERMINAL
E11k-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 410-k
A110-1
ELECT vi FROM LIST OF vj
[ENCRYPTION SERVER 410-k]
E11k-2
CREATE SECOND CONVERSION DATA (Gsk, Ysk, sk) AND SECOND CONVERSION-CERTIFICATE DATA (Guk, uk)
E11k-3
RETURN (Gsk, Ysk, sk) AND (Guk, uk) TO VOTER TERMINAL
E110-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
A110-5
CERTIFY INTRA-ORGANIZATION DIGITAL SIGNATURE Sei FOR (E(vi), (α, t), IIDi)
B110-6
TRANSMIT E (vi), (α, t) IIDi) AND Sei TO VOTING SERVER
[AUTHENTICATION SERVER]
B110-7
VERIFY LEGITIMACY OF Sei
A110-8
ACQUIRE COMMON-BASE IDENTIFIER CIDi CORRESPONDING TO IIDi
B110-9
CREATE DIGITAL SIGNATURE Sek OF AUTHENTICATION SERVER FOR (E (vi), (α, t), CIDi)
B110-10
TRANSMIT (E(vi), (α, t) CIDi) AND Sek TO VOTING SERVER

FIG.27

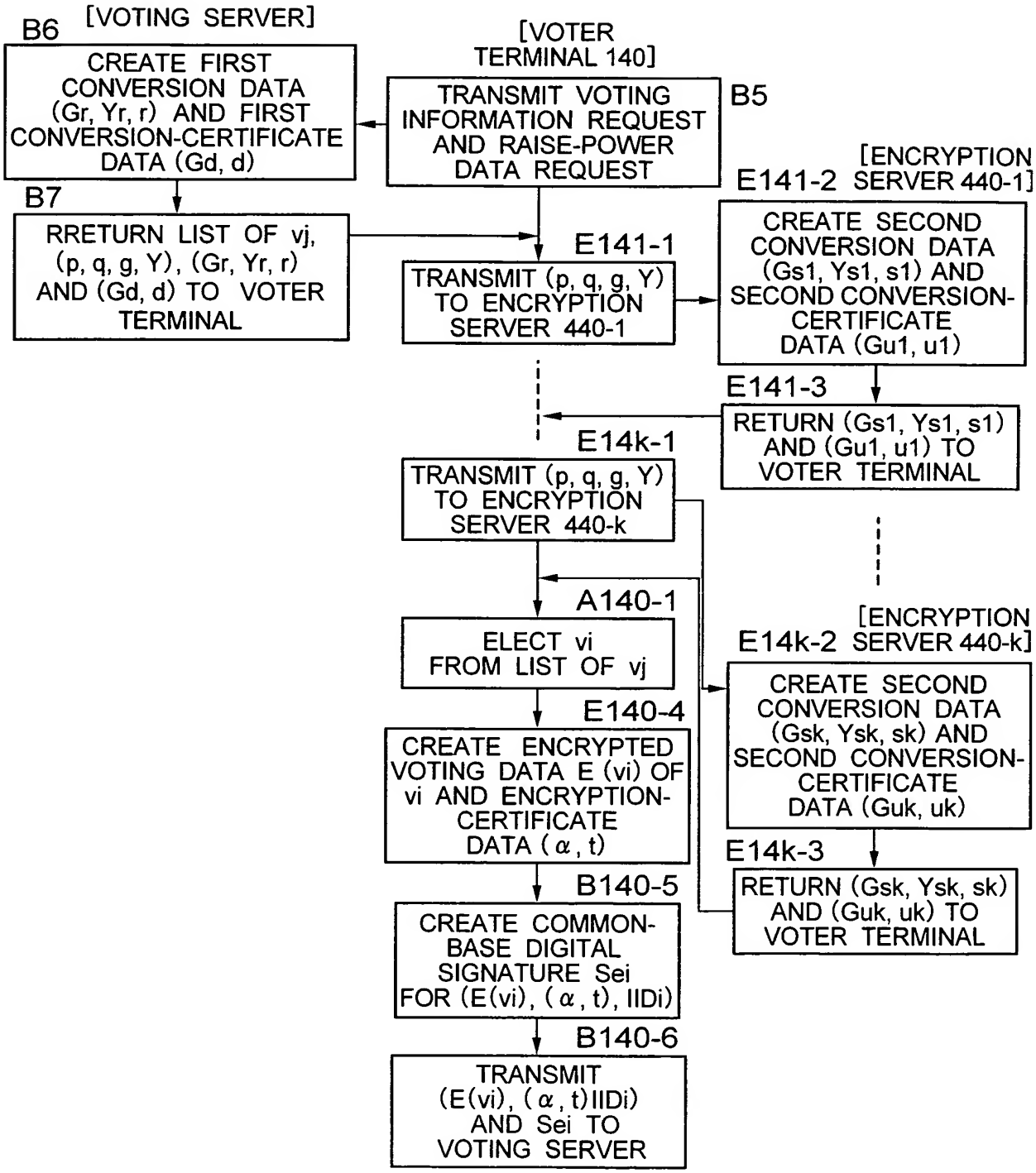
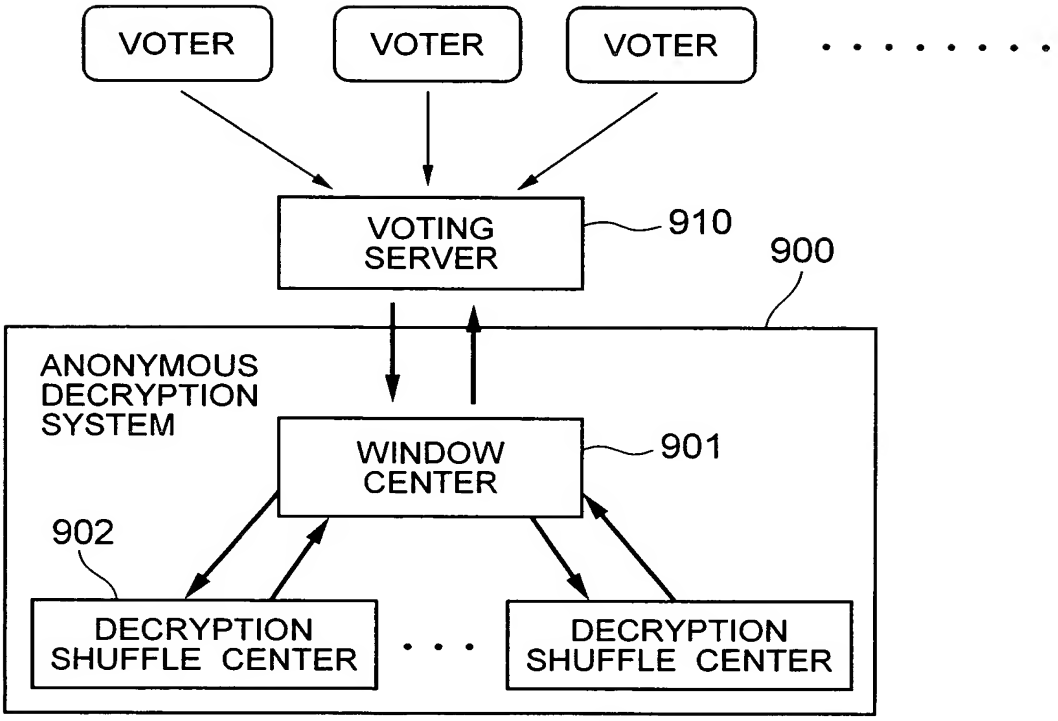

B6
[VOTING SERVER]
CREATE FIRST CONVERSION DATA (Gr, Yr, r) AND FIRST CONVERSION-CERTIFICATE DATA (Gd, d)
B7
RRETURN LIST OF vj, (p, q, g, Y), (Gr, Yr, r) AND (Gd, d) TO VOTER TERMINAL
[VOTER TERMINAL 140]
TRANSMIT VOTING INFORMATION REQUEST AND RAISE-POWER DATA REQUEST
B5
E141-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 440-1
[ENCRYPTION SERVER 440-1]
E141-2
CREATE SECOND CONVERSION DATA (Gs1, Ys1, s1) AND SECOND CONVERSION-CERTIFICATE DATA (Gu1, u1)
E141-3
RETURN (Gs1, Ys1, s1) AND (Gu1, u1) TO VOTER TERMINAL
E14k-1
TRANSMIT (p, q, g, Y) TO ENCRYPTION SERVER 440-k
[ENCRYPTION SERVER 440-k]
E14k-2
CREATE SECOND CONVERSION DATA (Gsk, Ysk, sk) AND SECOND CONVERSION-CERTIFICATE DATA (Guk, uk)
E14k-3
RETURN (Gsk, Ysk, sk) AND (Guk, uk) TO VOTER TERMINAL
A140-1
ELECT vi FROM LIST OF vj
E140-4
CREATE ENCRYPTED VOTING DATA E (vi) OF vi AND ENCRYPTION-CERTIFICATE DATA (α, t)
B140-5
CREATE COMMON-BASE DIGITAL SIGNATURE Sei FOR (E(vi), (α, t), IIDi)
B140-6
TRANSMIT (E(vi), (α, t)IIDi) AND Sei TO VOTING SERVER

FIG.28


VOTER
VOTER
VOTER
VOTING SERVER
910
900
ANONYMOUS DECRYPTION SYSTEM
WINDOW CENTER
901
902
DECRYPTION SHUFFLE CENTER
DECRYPTION SHUFFLE CENTER